А.В. Соколов, О.М. Степанюк

ЗАЩИТА ОТ КОМПЬЮТЕРНОГО ТЕРРОРИЗМА

- Проблемы защиты информации
- Характеристика угроз и способы защиты от них
- **Криптографическая** защита и биометрия
- Электронная цифровая подпись
- Стеганография

А. Соколов, О. Степанюк

Защита от компьютерного терроризма

Справочное пособие

БХВ-Петербург
Арлит
2002

Содержание

Введение

На современном этапе развития нашего общества многие традиционные ресурсы человеческого прогресса постепенно утрачивают свое первоначальное значение. На смену им приходит новый ресурс, единственный продукт не убывающий, а растущий со временем, называемый информацией. Информация становится сегодня главным ресурсом научно-технического и социально-экономического развития мирового сообщества. Чем больше и быстрее внедряется качественной информации в народное хозяйство и специальные приложения, тем выше жизненный уровень народа, экономический, оборонный и политический потенциал страны.

В настоящее время хорошо налаженная распределенная сеть информационно-вычислительных комплексов способна сыграть такую же роль в общественной жизни, какую в свое время сыграли электрификация, телефонизация, радио и телевидение вместе взятые. Ярким примером этому стало развитие глобальной сети Internet. Уже принято говорить о новом витке в развитии общественной формации — информационном обществе.

Любая предпринимательская деятельность тесно связана с получением, накоплением, хранением, обработкой и использованием разнообразных информационных потоков. Целостность современного мира как сообщества обеспечивается, в основном, за счет интенсивного информационного обмена. Приостановка глобальных информационных потоков даже на короткое время способно привести к не меньшему кризису, чем разрыв межгосударственных экономических отношений. Поэтому в новых рыночно-конкурентных условиях возникает масса проблем, связанных не только с обеспечением сохранности коммерческой (предпринимательской) информации как вида интеллектуальной собственности но и физических и юридических лиц, их имущественной собственности и личной безопасности.

Учитывая известный афоризм «цель оправдывает средства», информация представляет определенную цену. И поэтому сам факт получения информации злоумышленником приносит ему определенный доход, ослабляя тем самым возможности конкурента. Отсюда главная цель злоумышленника — получение информации о составе, состоянии и деятельности объекта конфиденциальных интересов (фирмы, изделия, проекта, рецепта, технологии и т. д.) в целях удовлетворения своих информационных потребностей. Возможно в корыстных целях и внесение определенных изменений в состав информации, циркулирующей на объекте конфиденциальных интересов. Такое действие может привести к дезинформации по определенным сферам деятельности, учетным данным, результатам решения некоторых задач. Более опасной целью является уничтожение накопленных информационных массивов в документальной или магнитной форме и про-

граммных продуктов. Полный объем сведений о деятельности конкурента не может быть получен только каким-нибудь одним из возможных способов доступа к информации. Чем большими информационными возможностями обладает злоумышленник, тем больших успехов он может добиться в конкурентной борьбе. На успех может рассчитывать тот, кто быстрее и полнее соберет необходимую информацию, переработает ее и примет правильное решение. От целей зависит как выбор способов действий, так и количественный и качественный состав привлекаемых сил и средств посягательства.

Одним из самых распространенных на сегодня источником получения информации являются компьютерные сети. Они постепенно превратились в такую же повседневность, как и телевидение или телефон. Множество компаний имеют свои собственные официальные страницы в Internet, подразделения компаний используют компьютерные сети для оперативного обмена коммерческой информацией, тысячи рядовых граждан используют сеть для получения важных для них данных (лент новостей, курсов валют и т.д.). Короче говоря, в Internet стала храниться и передаваться действительно важная информация (причем не только на Западе, но и у нас), стало обычной практикой подключение корпоративной компьютерной сети к Intermet, стало все больше пользователей, чей компьютер, обладая важной информацией, также используется и для работы в Intermet.

Кроме того, в последние годы всемирная компьютерная «паутина» становится эффективным средством совершения финансовых сделок и серьезным подспорьем в бизнесе. Согласно данным, проводимым исследовательской компанией International Data, объем Intermet-бизнеса достиг в 1999 году в США 74 млрд долларов, а в Европе — 19 млрд долларов. К 2003 году ожидается рост до 708 млрд и 430 млрд, соответственно. Объем отечественного Internet-бизнеса равен 15 млрд долларов.

Аналогичные процессы происходят сейчас и в России. У нас сохраняются самые высокие в Европе темпы продаж персональных компьютеров. Несмотря на низкое качество телефонных линий, рынок Intermet в нашей стране, по мнению экспертов, будет расширяться вдвое быстрее, чем в Западной Европе.

По словам бывшего директора Центрального разведывательного управления США Роберта Гейтса, возглавлявшего это учреждение с 1991 по 1993 год, в настоящее время безопасность конфиденциальной информации все чаще оказывается под угрозой, причем источников опасности становится все больше. Неприятностей можно ждать как со стороны организованных преступных синдикатов и террористов, так и от разведывательных центров, финансируемых правительством. Крупные компании, работающие в области высоких технологий, не должны строить никаких иллюзий, а руководители компаний должны помнить о существовании угрозы и предпринимать необходимые меры для обеспечения безопасности внутриведомственной информации.

Постоянные изменения в технологии и растущий спрос на компьютерную технику означают, что и преступность этого рода будет расти до тех пор, пока предприятия в срочном порядке не пересмотрят подход к проблемам безопасности и не усовершенствуют меры защиты. Компьютерная преступность — это противоправная и осознанная деятельность образованных людей и, следовательно, наиболее опасная для общества. Итак, западными специалистами и экспертами констатируется крайне тяжелое положение с информационной безопасностью в финансовых структурах, их неспособность, противостоять возможным атакам на информационные системы.

Любое компьютерное преступление представляет собой факт нарушения того или иного закона. Оно может быть случайным, а может быть специально спланированным; может быть обособленным, а может быть составной частью обширного плана атаки. Нанесение ударов по жизненно важным элементам, таким как телекоммуникации или транспортные системы предпринимаются экономическими противниками или террористическими группами.

Все мы привыкли считать, что терроризм — это взрыв машины, целого дома, захват заложников и т. д. Однако терроризм многолик и арсенал террористов неизмеримо шире. В ближайшем будущем терроризм будет распространяться в различных формах: воздушный терроризм всех видов, отравление продуктов питания, использование химического и биологического оружия, угроза нанесения ущерба ядерным объектам, АЭС; угроза разрушения плотин и затопления больших площадей и т. д. Все более широкое распространение получает террористическая деятельность в сфере информационных технологий, что может быть причиной многих техногенных катастроф. Появилось такое понятие, как «компьютерный или информационный» терроризм.

В наши дни любой банк, любая электростанция, любая транспортная сеть и любая телевизионная студия представляют собой потенциальную мишень для воздействия из киберпространства. Театр ведения информационных боевых действий простирается от секретного кабинета министра до домашнего персонального компьютера рядового пользователя.

Виртуальные террористы проникают в компьютерные системы, применяя «логические бомбы», вирусы, «троянских коней», электромагнитные импульсы и «радиочастотные пушки высокой мощности», которые учиняют опустошительную электронную «бурю» в компьютерной системе. Терроризм — государственный или любительский — связан с самыми сенсационными, громкими и ужасающими разрушениями, чего не скажешь, по мнению большинства людей, о «тихих» компьютерных диверсиях. Объектами нападок компьютерных мошенников становятся крупные корпоративные сообщества, а также фирмы и компании рангом пониже. У них, как правило, похищаются базы данных, а проще говоря — информация, предназначенная для сугубо внутреннего пользования. Цели воровства самые разные: от элементарного шантажа (например, с требованием выкупа) до мести недовольных сотрудников и полного разорения предприятия.

Прибегая к шантажу крупных корпораций или банков, злоумышленники знают, что последние постараются не поднимать «шума» и афишировать взлом своей компьютерной защиты. Заплатить дешевле. Не придется ни объясняться с общественностью, ни искать причины «прорыва обороны», ни устранять последствия. Сумма дани шантажистам приблизительно равна еженедельным эксплуатационным расходам любой из этих организаций.

В США для расследования случаев компьютерного вымогательства ФБР образовало три самостоятельных подразделения, которые расследуют деятельность компьютерных вымогателей. В качестве примера этого вида «деятельности» злоумышленников-кибергангстеров приведем следующие события, произошедшие в Лондоне за достаточно короткий промежуток времени:

- 6 января 1993 года деятельность одной из брокерских контор была полностью парализована после угрозы вымогателей и созданной ими аварийной ситуации в

компьютерной системе. Выкуп в размере 10 миллионов фунтов был переведен на счет в Цюрихе;

- 14 января 1993 года один из первоклассных банков выплатил вымогателям 12,5 миллионов фунтов;
- 29 января 1993 года одной из брокерских контор пришлось заплатить 10 миллионов фунтов отступного после аналогичных угроз;
- 17 марта 1995 года одна оборонная фирма была вынуждена откупиться 10 миллионами фунтов стерлингов.

Во всех четырех случаях компьютерные террористы угрожали высшим руководителям и демонстрировали имеющиеся у них возможности разрушить компьютерную систему. Все жертвы уступали требованиям вымогателей через несколько часов и переводили деньги на счета банков, располагающихся в офшорных зонах, откуда злоумышленники снимали их в считанные минуты.

На этапе подготовки операции использовались разнообразные методы сбора предварительной информации. Действуя под видом маркетинговых фирм, преступники тщательно изучали систему, выбранную объектом шантажа, опрашивая руководителей отделов информационных технологий. В некоторых случаях ничего не подозревающим руководителям даже вручали анкеты. Вооруженные полученной информацией, преступники могли взламывать системы безопасности и оставлять зашифрованные записки с обещаниями больших неприятностей. Считается, что кибер-террористы переняли опыт ведения информационных боевых действий у американских военных, которые разрабатывают «вооружение», способное выводить из строя или уничтожать компьютерную технику. Известно также, что некоторые банды просачивались в банки, устраивая диверсантов на временную работу.

Внешние атаки могут преследовать и более серьезные цели, чем пассивный сбор данных или шантаж, — такие, как, например, выведение из строя главных компьютерных узлов. По мнению экспертов, чтобы парализовать жизненно важные точки созданной инфраструктуры, достаточно нанести удар всего по нескольким десяткам объектов. Уже сегодня, по заявлениям некоторых иностранных экспертов, отключение компьютерных систем приведет к разорению 20% средних компаний и около 33% банков в течение нескольких часов, 48% компаний и 50% банков потерпят крах в течение нескольких суток.

Очень большие проблемы доставляют злоумышленники и обладателям кредитных карточек (воришки похищают их номера, чтобы потом использовать по собственному усмотрению), а также и рядовым гражданам, не имеющим никакого отношения ни к бизнесу, ни к хранению денег на пластиковых картах.

Обычно когда речь заходит о безопасности компании, ее руководство недооценивает важность информационной безопасности. Основной упор делается, как правило, на физической защите. Крепкие входные двери, защищенные окна, разнообразные датчики и видеокамеры, надежная служба охраны — эти компоненты помогут предупредить угрозу взлома рабочего помещения. Но как предотвратить компьютерный «взлом»? Для того чтобы проникнуть в тайны компании, нет необходимости перелезать через заборы и обходить периметровые датчики, вторгаться в защищенные толстыми стенами помещения, вскрывать сейфы и т. п. Достаточно проникнуть в информационную систему и перевести сотни тысяч долларов на чужие счета или вывести из

строя какой-либо узел корпоративной сети. Все это приведет к огромному ущербу. Причем не только к прямым потерям, которые могут выражаться цифрами со многими нулями, но и к косвенным. Например, выведение из строя того или иного узла приводит к затратам на обновление или замену программного обеспечения. А атака на публичный Web-сервер компании и замена его содержимого на любое другое может привести к снижению доверия к фирме и, как следствие, потере части клиентуры и снижению доходов. Системы физической защиты имеют аналоги в мире информационной безопасности локальных вычислительных сетей, функцию стальной двери выполняет межсетевой экран. Традиционно он ограждает внутреннюю сеть от внешних несанкционированных вмешательств. Существует несколько систем сетевой защиты, например, такие как Firewall или Broundmouer. Они контролируют все входящие и исходящие соединения между защищаемым сегментом локальной сети и сети Internet. Одним из элементов защиты является криптографирование, т. е. шифрование информации, которая передается по открытым каналам связи.

По мнению большинства наших сограждан, основная опасность исходит от «хакеров», внешних злоумышленников, которые проникают в компьютерные системы банков и военных организаций, перехватывают управление спутниками и т. д. Стоит только вспомнить публикации о российских «профессионалах-одиночках», которые проникали в компьютерные сети Пентагона, крали важнейшую информацию с грифом «TOP SECRET» и оставляли после себя надписи: «Здесь был Вася!». Вот тут-то и надо четко усвоить: если вы подключились к Internet, то не только он стал открытым для вас, но и вы вывернули для него наизнанку свой компьютер.

Безусловно, опасность вмешательства извне весьма актуальна. Но она слишком уж преувеличена. Статистика свидетельствует, что до 70—80% всех компьютерных преступлений связаны с внутренними нарушениями. Доказано, что именно некорректные или сознательно провокационные действия персонала становятся причиной нарушения работы сети, утечек информации и, в конечном счете, финансовых и моральных потерь предприятия. В качестве примера напомним случай на Игналинской АЭС, когда местный системный программист внедрил во внутреннюю сеть программную закладку («троянского коня», которая чуть не привела к аварии на станции. Именно для предупреждения подобных ситуаций существуют различные системные анализаторы.

В настоящее время, когда не только взломщики «по призванию», но и государственные органы (налоговая полиция, например) пытаются вмешиваться в информационную деятельность компаний и фирм, вышеназванные меры предосторожности просто необходимы. Поэтому лучше поставить надежный барьер постороннему влиянию, чем потом бороться с нежелательными последствиями.

В современном мире мощь страны определяется в первую очередь ее экономическими возможностями, поэтому многочисленные разведывательные службы уделяют вопросам бизнеса все более серьезное внимание. Правительства финансируют операции, в ходе которых изучается финансовая деятельность различных компаний, собираются сведения о намечающихся контрактах, сообщается информация о финансовом положении организаций и банковских операциях, анализируются события, которые могут отразиться на формировании цен на мировых рынках.

Для получения важных сведений разведывательные службы активно используют многочисленные методы, разработанные в период холодной войны. К этим методам

можно отнести, например прослушивание телефонных разговоров и анализ документов, оставленных бизнесменами в номерах гостиниц в ходе деловых поездок. Разведслужбы внедряют в компании агентов, которые крадут или тайком копируют файлы с недостаточно защищенных компьютеров. Некоторые подразделения имеют в своем распоряжении сложные средства перехвата, позволяющие расшифровать даже закодированную информацию, пересылаемую по корпоративным каналам связи. Особенно уязвимы сообщения, зашифрованные с использованием устаревших технологий. Секретные ведомства регулярно анализируют телекоммуникационный трафик, а также информацию, пересылаемую между компьютерами, в том числе и электронную почту.

В настоящее время мир озабочен состоянием защиты национальных информационных ресурсов в связи с расширением доступа к ним через открытые информационные сети типа Internet. Кроме того, что повсеместно увеличивается число компьютерных преступлений, реальной стала угроза информационных атак на более высоком уровне для достижения политических и экономических целей.

К наиболее уязвимым местам, через которые обычно пытаются проникнуть злоумышленники, относятся открытые системы, системы, поддерживающие технологию подключения периферийных устройств в режиме plug-and-play, средства централизованной удаленной поддержки, коммутируемые каналы удаленного доступа и недостаточно надежные технологии шифрования. В то же время компании вполне в состоянии обеспечить достаточно надежную защиту информации при относительно небольших затратах.

Нормальная жизнедеятельность общественного организма целиком определяется уровнем развития, качеством функционирования и безопасностью информационной среды. Производство и управление, оборона и связь, транспорт и энергетика, финансы, наука и образование, средства массовой информации — все зависит от интенсивности информационного обмена, полноты, своевременности, достоверности информации. Именно информационная инфраструктура общества — мишень информационного терроризма. Не стоит утешать себя тем, что ввиду унаследованной информационной замкнутости, определенной технологической отсталости Россия менее уязвима, чем другие государства. Скорее наоборот. Как раз высокая степень централизации структур государственного управления российской экономикой может привести к гибельным последствиям в результате информационной агрессии или террористических действий. Конечно, наши спецслужбы располагают необходимыми средствами и известным опытом предотвращения перехвата, утечек, искажений, уничтожения информации в информационных и телекоммуникационных сетях и системах общегосударственного назначения. Но темпы совершенствования информационного оружия (как, впрочем, и любого вида атакующего вооружения) превышают темпы развития технологий защиты. Вот почему задача нейтрализации информационного оружия, парирования угрозы его применения должна рассматриваться как одна из приоритетных задач в обеспечении национальной безопасности страны.

Руководителям компаний следует уделять особое внимание защите наиболее важных направлений своего бизнеса (в частности, научно-исследовательские работы), инструктировать сотрудников, использующих мобильные компьютеры, предупреждать их о необходимости проведения профилактических мероприятий для предотвращения

кражи информации. Нужно оснастить телекоммуникационные системы коммерчески доступными средствами шифрования, уже получившими всеобщее распространение и хорошо зарекомендовавшие себя с точки зрения надежности. К примеру, на взлом алгоритма шифрования, недавно одобренного министерством торговли США, по оценке экспертов, уйдет не менее 149 трлн лет. Хотя с такими высокими темпами развития компьютерных технологий, как сейчас, вполне возможно, что лет через 10 время взлома этого алгоритма значительно сократится. И, вообще, быть абсолютно уверенным в защищенности вашей информации никогда нельзя, так как наравне с разработкой методов шифрования и защиты информации разрабатываются и методы их взлома. Например, существуют компании, занимающиеся проверкой надежности защищенности информации. Сотрудниками этих компаний могут быть как специалисты по защите информации, так и профессиональные хакеры, перешедшие на сторону не взлома, а защиты. Также не абсолютную надежность систем защиты информации и шифрования подтверждают и сообщения о взломах различных программ и операционных систем хакерами. Например, два выдающихся израильских хакера повергли в шок специалистов по защите информации, заявив, что они нашли способ извлечь криптографические ключи DES из персональных компьютеров и смарт-карт. Ади Шамир, один из трех авторов разработки методологии шифрования с открытыми ключами, и Эли Бихам утверждают, что они могут получить даже 168-разрядный секретный ключ Triple-DES. 56-разрядный стандарт DES использовался до 2001 года в США для использования в банковской сфере и широко реализован в программных и аппаратных продуктах, и именно после того, как стала найдена методика расшифровки этого стандарта, США отказались от использования стандарта DES.

Кроме того, необходимо физически ограничить доступ посторонних лиц к наиболее ответственным данным и приложениям и следить за регулярной сменой паролей. Все это очевидно, но известно, что на практике данные правила соблюдаются крайне редко. Прежде всего необходимо отделить информацию, имеющую критически важное значение для технологии производства продукции, проведения научно-исследовательских работ, осуществления финансовых операций и реализации маркетинговой стратегии, и гарантировать ее надежную защиту.

Руководители компаний должны постоянно помнить о существовании угрозы и предпринимать необходимые меры для обеспечения безопасности. Это позволит укрепить завоеванные позиции, даже если ваша компания не является непосредственным объектом интереса государственных разведывательных служб, конкурентов, криминальных организаций, террористов или хакеров.

Предлагаемый в настоящем пособии материал ориентирован, прежде всего, на практические задачи обеспечения безопасности информации и охватывает основные стадии их решения от оценки угрозы до реализации систем защиты, а также некоторые правовые аспекты информационной безопасности.

В первой главе книги дана характеристика современного состояния безопасности информации. Дан анализ компьютерных преступлений и приведены типовые способы атак на информацию в сети. А также описана модель нарушителя безопасности информации.

Вторая глава посвящена проблемам защиты информации. Даны характеристики угроз безопасности информации и подробно описаны возможные несанкционирован-

ные действия в отношении к компьютерам, сетевым ресурсам и каналам связи. Рассмотрены воздействие вредоносного программного обеспечения и силовые разрушительные воздействия на информацию, циркулирующую в компьютерных системах.

В третьей главе рассматриваются основные пути обеспечения информационной безопасности. В ней изложена концепция защиты информации и рассмотрены виды ее обеспечения. Определены методы и средства защиты информации от различных атак.

Методы криптографической защиты информации рассматриваются в четвертой главе этой книги. В ней даны основные определения криптографии. Подробно описаны способы шифрования в сети и основные криптографические протоколы. Рассмотрены принцип функционирования и использование электронной почты и электронной цифровой подписи.

Последняя, пятая глава, посвящена компьютерной стеганографии. В ней рассмотрены принципы построения стеганографии и дан анализ путей ее практической реализации.

В Приложении приведены основные термины, определения и сокращения, которые используются в различной литературе, посвященной вопросам защиты информации и компьютерным системам.

Авторы не стремились излагать материал как полные знания, необходимые специалистам, что и невозможно в таком небольшом объеме, а главным образом постарались через этот материал дать представление об основных направлениях и методах защиты информации, которые реально используются или могут быть использованы в ближайшее время.

Надеемся, что бизнесмены, юристы, да и просто люди, по разным причинам ставшие носителями коммерческих или других секретов, получат представление о реальных возможностях информационных террористов и мерах противодействия им.

ГЛАВА 1. СОВРЕМЕННОЕ СОСТОЯНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Безопасность — аспект нашей жизни, с которым нам приходится сталкиваться ежедневно: двери закрываем на ключ, ценные вещи убираем от посторонних глаз и не оставляем бумажники где попало. Это должно распространяться и на «цифровой мир», потому что компьютер каждого пользователя может оказаться объектом пиратского нападения.

Коммерческие организации всегда считали затраты на обеспечение безопасности неизбежным злом, а не своим первоочередным делом. До известной степени это «мудро»: в конце концов, и без того достаточно препятствий для выполнения работы, чтобы еще создавать новые. Однако много ли вы видели «капитанов индустрии», находящихся в здравом уме, которые бы отважились разрешить круглосуточный свободный доступ во все корпоративные помещения своей фирмы? Конечно же, нет! У входа в помещение даже небольшой компании вас встретит охранник или система ограничения и контроля доступа. А вот с защитой информации дела обстоят еще не так хорошо. Не все понимают, как можно потерять информацию и во что это выльется.

Крупные игроки уже получили хороший урок: хакеры нанесли большой ущерб таким компаниям, как Yahoo!, Amazon corn и даже Агентству космических исследований NASA. Монстр RSA Security (один из крупнейших поставщиков на рынке услуг безопасности) подвергся атаке через несколько дней после необдуманного заявления о наличии противоядия против любых угроз.

Профессионалы, искушенные в проблемах безопасности, делят угрозы, исходящие от людей или предметов и причиняющие вред, на следующие классы: *внутренние* или *внешние* и *структурированные* (против определенного объекта) или *неструктурированные* (адресуемые по принципу — «кому Бог пошлет»). Например, компьютерные вирусы классифицируются как «внешние неструктурированные угрозы» и являются вполне обычными. Удивительно, что пользователи не считают свой компьютер конкретной мишенью, они чувствуют себя более защищенными.

Степень необходимой защиты во многом зависит от состояния ваших дел. Если ваша организация или компания является мишенью для политического давления, если вы входите в состав государственной или системообразующей инфраструктуры, распределяющей национальные энергетические ресурсы или обслуживающей нацио-

нальные сети связи, то обычные террористы могут отложить в сторону свои бомбы и пистолеты и рассматривать возможность электронной атаки на вашу организацию, применяя разнообразные программные средства.

С другой стороны, если речь идет об обычной организации по продажам и маркетингу, то вам придется побеспокоиться лишь о ваших сотрудниках, ворующих списки клиентов; о мошенниках, приобретающих товары по фальшивым кредитным карточкам, о конкурентах, проникающих в вашу сеть с целью получения доступа к прейскурантам, о хакерах, взламывающих ваш Web-сайт с целью вымогательства, и т. п.

Однако не надо паники. Есть хорошие новости: безопасность не всегда заключается в трате целого состояния на новейший «черный ящик». Повседневные меры предосторожности — это как раз то, что нужно использовать в первую очередь. Наиболее популярный способ получения информации — обычная кража. Вы же не оставляете на своем письменном столе на ночь тысячу долларов наличными (если они у вас есть), так почему бы не уделить немного времени обеспечению безопасности своего кормильца — персонального компьютера? Это касается не только аппаратных средств, но и данных, кража или потеря которых наносит большой, порой непоправимый, ущерб.

Многие руководители, возможно, скажут, что самыми широкими правами доступа к важным для компании данным обладают только они и их коллеги вместе с адвокатами и бухгалтерами. Они ошибаются! Доступом ко всем конфиденциальным материалам всех трех групп обладают системные администраторы. Более того, как правило, они не имеют долевого участия в прибылях компании или «золотых наручников». Поэтому именно они представляют собой одну из самых больших потенциальных угроз для безопасности организации. Следует заметить, что компании тщательно проверяют людей, поступающих на эту работу. Попробуйте сделать это, и вы наверняка будете поражены результатами, когда узнаете, кому вы доверили всю информацию. Также внимательно следует присмотреться и к поставщикам услуг безопасности, особенно к тем, кто предлагает консультирование, планирование и администрирование.

Одно из последних веяний моды — поиск на должность администратора сети «перебесившихся компьютерных хулиганов». Кто лучше бывшего хакера сможет поддерживать и тестировать безопасность компьютерной сети и давать необходимые рекомендации? В такой формулировке перспективы выглядят вполне радужно. Однако есть и другая сторона медали. Дать привилегированный доступ к конфиденциальной информации о структуре сети и местонахождении наиболее важных данных криминальному элементу, который, с одной стороны, подкован технически, а с другой, не приспособлен к серьезной и кропотливой работе по обеспечению безопасности — есть, над чем подумать.

Когда электронная коммерция, электронный бизнес и электронная «всякая всячина» продолжают разрастаться как снежный ком, значительно возрастает риск, связанный с безопасностью. Чем выше наша зависимость от систем жизнеобеспечения, тем больше внимания необходимо уделять их защите. Насколько хорошо защищена ваша сеть? Чтобы правильно ответить на этот банальный вопрос, нужно обладать некоторыми знаниями. В этом вам поможет книга, которую вы держите в руках.

Опасность информационных войн и кибератак

На современном этапе развития цивилизации информация играет ключевую роль не только в функционировании общественных и государственных институтов, но и в жизни каждого человека. На наших глазах информатизация общества развивается стремительно и зачастую непредсказуемо, а мы лишь начинаем осознавать его социальные, политические, экономические и другие последствия. Информатизация нашего общества ведет к созданию единого мирового информационного пространства, в рамках которого производится накопление, обработка, хранение и обмен информацией между субъектами этого пространства — людьми, организациями, государствами.

Очевидно, что возможности быстрого обмена политической, экономической, научно-технической и другой информацией, применение новых технологий во всех сферах общественной жизни и особенно в производстве и управлении является несомненным благом. Однако быстрое развитие промышленности стало угрожать экологии Земли, а достижения в области ядерной физики породили опасность ядерной войны. Информатизация тоже может стать источником серьезных проблем.

Всем давно известно широко распространенное очень лаконичное и вместе с тем емкое определение понятия «война», которое дал фон Клаузевиц — один из выдающихся военных теоретиков XIX века. Он сказал, что война — это продолжение политики другими средствами, когда перо дипломата меняется на штык военного. Так было на протяжении всей истории человечества.

Войны происходили всегда. В период, когда еще не было государств, они сводились просто к грабежу соседей. С развитием государств бандитские налеты получают державное благословение и превращаются в очень почетное ремесло. Целые цивилизации возникли, выросли, состарились и погибли на войне. Со временем ведение войны превратилось в целую науку. И, как у всякой уважающей себя науки, у войны появились своя история, свои правила, выдающиеся представители, своя методология. Каждый народ привносил в эту науку что-то оригинальное, даже если оно выглядело жалким на фоне других вкладов. Технический прогресс во все времена был самым верным спутником войны. Как говорится — война есть двигатель прогресса.

Современная военная мысль шагнула далеко вперед. Теперь ее сфера — весь земной шар. Из локализованного разбойничьего налета война превратилась в глобальную проблему, которая может разрушить не одно государство. И хотя это практически всем известно, война по-прежнему заставляет служить ей верой и правдой, не за страх, а за совесть многие выдающиеся умы человечества.

В военных доктринах разных стран мира все чаще обнаруживаются упоминания о программах развития электронного оружия и программного обеспечения специального назначения. В результате анализа информации, поступающей из различных разведывательных источников, можно сделать вывод, что правительства некоторых государств активно финансируют разработку наступательных кибер-программ. Информационная война рассматривается в качестве возможной стратегической альтернативы в тех странах, где понимают, что при ведении боевых действий обычными средствами они явно уступают.

Сам термин *информационная война* обязан своим происхождением военным и обозначает жестокую и опасную деятельность, связанную с реальными, кровопролитными и разрушительными боевыми действиями. Военные эксперты, сформулировавшие доктрину информационной войны, отчетливо представляют себе отдельные ее грани: это штабная война, электронная война, психологические операции и т. д.

Информационная война включает действия, предпринимаемые для достижения превосходства в обеспечении национальной военной стратегии путем воздействия на информационные системы противника и одновременное укрепление и защиту собственных.

Информационная война представляет собой всеобъемлющую целостную стратегию, призванную отдать должное значимости и ценности информации в вопросах командования, управления и выполнения приказов вооруженными силами и реализации национальной политики. Такая война нацелена на все возможности и факторы уязвимости, неизбежно возникающие при возрастающей зависимости от владения информацией, а также на использование информации во всевозможных конфликтах.

Объектом внимания становятся информационные системы (включая линии передач, обрабатывающие центры и человеческие факторы этих систем), а также информационные технологии, используемые в системах вооружений. Крупномасштабное противостояние между общественными группами или государствами имеет целью изменить расстановку сил в обществе. Информационная война включает наступательные и оборонительные составляющие.

Под *угрозой информационной войны* понимается намерение определенных сил воспользоваться возможностями компьютеров на необозримом виртуальном пространстве, чтобы вести «бесконтактную» войну, в которой количество жертв (в прямом значении слова) сведено до минимума. «Мы приближаемся к такой ступени развития, когда уже никто не является солдатом, но все участвуют в боевых действиях, — сказал один из руководителей Пентагона. — Задача теперь состоит не в уничтожении живой силы, но в подрыве целей, взглядов и мировоззрения населения, в разрушении социума».

Поскольку современная информационная война связана с вопросами использования информации и коммуникаций, то, если смотреть в корень, это война за знания о себе и противниках.

Электронный удар, нанесенный по одной из важных стратегических целей (например, по центру управления перевозками или пункту распределения электроэнергии), по своим разрушительным последствиям может оказаться гораздо эффективнее применения оружия массового поражения.

Как заявил представитель Центрального разведывательного управления Джон Серабьян, Соединенные Штаты недостаточно защищены от электронных атак террористов и иностранных государств. «В военных доктринах разных стран мира все чаще обнаруживаются упоминания о программах развития электронного оружия и программного обеспечения специального назначения, — подчеркнул Серабьян. — В результате анализа информации, поступающей из различных разведывательных источников, мы пришли к выводу, что правительства некоторых государств активно финансируют разработку наступательных киберпрограмм. Информационная война рассматривается в качестве возможной стратегической альтернативы в тех странах, где понимают, что при ведении боевых действий обычными средствами они явно уступают Соединенным Штатам».

И хотя среди вероятных источников угрозы США называют Россию и Китай, но есть информация, что кибератаки могут исходить и от других государств.

Любая война, в том числе и информационная, ведется с использованием современного оружия. Информационное оружие принципиально отличается от всех других средств ведения войны тем, что с его помощью могут вестись (и уже ведутся) необъявленные и чаще всего невидимые миру войны и что объектами воздействия этого оружия являются гражданские институты общества и государства: экономические, политические, социальные и т. д. Уже признано, что сети передачи данных превращаются в поле битвы будущего.

Информационное оружиеможет использоваться с «электронными скоростями» при нападении и обороне. Оно базируется на самых передовых технологиях и призвано обеспечить разрешение военных конфликтов на ранней стадии, а также исключить применение сил общего назначения. Стратегия применения информационного оружия носит наступательный характер. Однако есть понимание собственной уязвимости, особенно гражданского сектора, поэтому проблемы защиты от такого оружия и информационного терроризма сегодня выходят на первый план. Последнее обстоятельство следует помнить руководству многих российских государственных и корпоративных сетей, которые уже активно работают в Internet и намерены подключаться к другим глобальным телекоммуникационным сетям. Уязвимость национальных информационных ресурсов стран, обеспечивающих своим пользователям работу в мировых сетях, — вещь обоюдоострая. Информационные ресурсы противников взаимно уязвимы.

Теоретики нередко относят к этому виду оружия различные способы информационного воздействия на противника: от дезинформации и пропаганды до радиоэлектронной борьбы. Однако информационным оружием точнее было бы назвать средства уничтожения, искажения или хищения информационных массивов, средства преодоления систем защиты, ограничения допуска законных пользователей, дезорганизации работы аппаратуры и компьютерных систем в целом. Атакующим информационным оружием сегодня можно назвать:

- *компьютерные вирусы,* способные размножаться, внедряться в программы, передаваться по линиям связи, сетям передачи данных, выводить из строя системы управления и т. п.;
- *логические бомбы* — запрограммированные устройства, которые внедряют в информационно-управляющие центры военной или гражданской инфраструктуры, чтобы по сигналу или в установленное время привести их в действие;
- *средства подавления информационного обмена в телекоммуникационных сетях,* фальсификация информации в каналах государственного и военного управления;
- *средства нейтрализации тестовых программ*;
- *ошибки* различного рода, сознательно вводимые лазутчиками в программное обеспечение объекта.

Универсальность, скрытность, различие способов программно-аппаратной реализации, радикальность воздействия, возможность выбора времени и места применения, наконец, экономичность делают информационное оружие чрезвычайно опасным: его легко замаскировать под средства защиты, скажем, интеллектуальной

собственности; кроме того, оно позволяет даже вести наступательные действия анонимно без объявления войны.

Оборонно-разведывательное агентство США опубликовало отчет о расследовании источников кибератак на национальные сайты. Результаты удивили американских военных: 80% хакерских атак приходится с территории Канады. Данные отчета были специально отправлены в департамент национальной обороны Канады. Еще до появления этого отчета директор ФБР Луис Фрих назвал Канаду *приютом хакеров.* Фрих подчеркнул свою уверенность в том, что канадские кибервандалы приняли непосредственное участие в нападениях на сайты Yahoo!, eBay, CNN и т. д. Федеральными властями США доказано, что в этих атаках использовались канадские серверы.

По сообщению Yahoo! Actialites, информационные пираты, следы которых ведут в Швецию, украли программу спутниковой навигации американского флота. Интересно, что хакеры использовали при этом компьютерную сеть немецкого университета Kaiserslautern, работая во время рождественских каникул 2000 года.

Учебное заведение подтвердило информацию, уже распространяемую местной радиостанцией SWR4, что хакеры нанесли ущерб на огромную сумму. Одна лишь лицензия на использование навигационной программы в течение года стоит $60 млн. С другой стороны, это может иметь серьезнейшие последствия с точки зрения военной, так как похищенная программа предусматривает возможность спутникового пилотирования различных систем слежения.

Один из китайских генералов высказал следующую мысль: «Мы вполне могли бы парализовать командный пункт противника, который при получении дезинформации будет принимать неверные решения. У нас есть возможность установить контроль над национальной банковской системой противника и над обществом в целом».

Изощренные попытки взломать компьютеры Пентагона, предпринимавшиеся на протяжении трех лет, вероятно, были совершены с ведома властей российскими хакерами, сообщает MSNBC.com.

Консультант Национального агентства безопасности (NSA) Джеймс Адаме (James Adams) сообщил, что американские дипломаты заявили свой официальный протест российскому правительству после того, как в 2001 году в результате расследования было обнаружено, что атаки хакеров под кодовым названием «Лунный лабиринт» велись с семи российских Internet-адресов. Но российские официальные лица заявили, что телефонные номера, с которых якобы были осуществлены атаки, тогда не действовали и у них нет информации об атаках, предпринятых против сайтов Пентагона.

Однако атаки не ослабевают. Кибератаку «Лунный лабиринт» Адаме оценивает «как самое настойчивое и серьезное наступление на Соединенные Штаты». Эта атака вызвала крупномасштабное расследование. Представитель Госдепартамента сообщил, что в связи с этими продолжающимися атаками были даже предприняты попытки обвинить Россию в компьютерном шпионаже.

Впервые «Лунный лабиринт» зафиксировали в марте 1998 года, когда сетевые администраторы заметили: кто-то зашел на один из сайтов Пентагона, замаскировав атаку таким образом, что сетевым администраторам оказалось довольно сложно зафиксировать вторжение.

Несмотря на все усилия, предпринятые для расследования этого громкого дела, до сих пор так и не ясно, кто же предпринял эти атаки. На данной стадии расследова-

ния атаки приписываются иностранным организациям, что может повлечь полномасштабный конфликт, если атаки хакеров спонсируются правительством иностранной державы.

Интересно, что как Китай, так и Россия проявляют интерес к любым формам сотрудничества с другими государствами, которое могло бы воспрепятствовать подобным атакам. Россия официально обратилась к Генеральному секретарю ООН с просьбой разработать свод международных законов, с помощью которых можно было бы эффективно бороться с преступлениями и терроризмом на информационном фронте.

Кибероружие— очень мощное стратегическое средство в руках тех стран, которые уступают в обычном вооружении. Эти страны понимают, что успешная кибератака, проведенная внутри или за пределами страны вероятного противника, может существенно укрепить их позиции в случае вооруженного конфликта. Учитывая растущую киберугрозу, нужно принимать соответствующие меры, внося коррективы в порядок функционирования киберпространства, которое оказывает все большее влияние на развитие бизнеса.

Приказ о начале подготовки к электронной атаке возможных противников, которые запасаются кибероружием, был отдан командованием армии США и одобрен еще президентом Клинтоном и министром обороны США Уильямом Коэном. Эта атака, вероятнее всего, будет включать в себя массированные нападения DDoS, распространение вирусов и »троянских коней», а также генерацию помех на соответствующих радиочастотах. Однако, как говорят американские военные, у армии нет возможности произвести такую атаку сейчас. «Мы видим три основные угрозы — баллистические ракеты, кибератаки и контроль над космическим пространством», — сказал генерал-лейтенант Эдвард Андерсон, представитель главнокомандующего в Командовании космическими силами, которому и было поручено возглавить создание стратегии кибернападения.

«Технология проведения кибератак достаточно хорошо изучена, — отметил профессор военной стратегии и национальной безопасности финансируемого Пентагоном Национального университета обороны Дэниел Кюль. — Те средства, которые кибер-вандалы применили несколько недель назад (речь идет об атаке на ряд крупных Web-узлов), могут быть использованы в гораздо более широких масштабах для нанесения ударов по объектам национальной экономики и инфраструктуры».

Кибератакам подвержены и сайты других стран. Согласно данным независимых экспертов из Everyday People, за первые 5 месяцев 2001 года совершено уже около 650 нападений на японские Web-сайты. За весь 2000 год, сообщает Ananova.com, было предпринято всего 63 нападения.

Киберпротесты достигли своего пика в марте 2001 года, когда официальный сайт Министерства образования, культуры, спорта, науки и технологии был закрыт из-за потоков враждебно настроенного трафика из Южной Кореи. Камнем преткновения послужили планы правительства Японии изменить школьную программу. Протестующие уверяют, что новые школьные учебники обеляют сомнительные события времен Второй мировой войны. Атаки оказались настолько существенными, что японское правительство было вынуждено официально обратиться к Южной Корее с просьбой принять меры против хакеров. Учебник же был издан с некоторыми изменениями.

Приведенные примеры свидетельствует о том, что сейчас как никогда актуальна проблема информационного вторжения в компьютерные сети с применением информационного оружия. Выход этой угрозы на первый план связан с тем, что современные системы управления являются системами критических приложений с высоким уровнем компьютеризации. Они могут оказаться весьма уязвимыми с точки зрения воздействия информационного оружия в военное и мирное время. Такое воздействие может привести к тому, что к угрожаемому периоду (перед вооруженным конфликтом) оружие сдерживания страны, подвергшейся агрессии, за счет скрытого внедрения закладок в программное обеспечение систем управления окажется полностью или частично заблокированным. О реальности этого утверждения свидетельствует опыт войны в Персидском заливе. Ирак практически не смог применить закупленные во Франции системы ПВО потому, что их программное обеспечение содержало логические бомбы, которые были активизированы с началом боевых действий.

Какая операционная система установлена на вашем компьютере? Скорее всего, одна из разновидностей Windows, как и на компьютерах ваших друзей, знакомых, вашего предприятия. К этому программному продукту все привыкли, все от него зависят. А это значит, что и Windows можно рассматривать как одно из проявлений информационного оружия. Никто не хочет оказаться в информационной или телекоммуникационной зависимости, но никто пока не знает, как этого избежать.

Американские военные считают, что преимущество в информационном оружии должно упрочить мировое лидерство США. Этим объясняется большой интерес и активность американцев в исследовании проблем информационной войны. Все сказанное подтверждается докладами и дискуссиями на международных конференциях по информационной войне, большинство участников которых составляют сотрудники государственных учреждений, армии и разведывательного сообщества США — АНБ, ЦРУ, ФБР.

Не многим известно, что вот уже несколько лет ведущие высшие учебные заведения армии США, в частности, Национальный университет обороны в Вашингтоне и Военно-морской колледж в Ньюпорте, выпускают таких военных профессионалов, как специалисты по информационной войне (по штатному расписанию — infowar officers). Другое, не менее могущественное ведомство, ЦРУ, уже несколько лет выполняет сверхсекретную программу по внедрению во все чипы, производимые американскими компаниями для мощных компьютерных систем как на территории США, так и за ее пределами, логических бомб, которые при получении особого сигнала (например, со спутника) могут вызывать сбои в работе этих систем или вовсе выводить их из строя. При этом нет открытых данных о новейших методах ведения военных действий и вообще о принципиально новом оружии — информационном. Отсутствуют полные данные и о масштабах информационного терроризма, который в последние два-три года приобрел уже глобальный характер (есть сведения о том, что некоторые террористические организации получили возможность использовать в своих целях даже *спутниковые транспондеры* — каналы, через которые можно манипулировать информацией).

К сожалению, иностранные специалисты первыми поняли и оценили значение информационного оружия, что послужило поводом к разработке стратегической концепции строительства вооруженных сил стран НАТО, в основу которой положено обес-

печение информационного превосходства над противником на всех стадиях развития конфликта — «Единая перспектива 2010» *(Joint Vision 2010)*.

В современном обществе военная стратегия использования информационного оружия оказалась тесно связанной с гражданским сектором и стала во многом от него зависеть. Разнообразие информационного оружия, форм и способов его воздействия, особенности появления и применения породили сложнейшие задачи защиты от него.

Считается, что для предотвращения или нейтрализации последствий применения информационного оружия необходимо принять следующие меры:

- защита материально-технических объектов, составляющих физическую основу информационных ресурсов;
- обеспечение нормального и бесперебойного функционирования баз и банков данных;
- защита информации от несанкционированного доступа, ее искажения или уничтожения;
- сохранение качества информации (своевременности, точности, полноты и необходимой доступности).

Создание технологий обнаружения воздействий на информацию, в том числе в открытых сетях, — это естественная защитная реакция на появление нового оружия. Экономическую и научно-техническую политику подключения государства к мировым открытым сетям следует рассматривать через призму информационной безопасности. Будучи открытой, ориентированной на соблюдение законных прав граждан на информацию и интеллектуальную собственность, эта политика должна предусматривать защиту сетевого оборудования на территории страны от проникновения в него элементов информационного оружия. Это особенно важно сегодня, когда осуществляются массовые закупки зарубежных информационных технологий.

Понятно, что без подключения к мировому информационному пространству страну ожидает экономическое прозябание. Оперативный доступ к информационным и вычислительным ресурсам, поддерживаемым сетью Internet, разумеется, следует приветствовать как фактор преодоления международной изоляции и внутренней дезинтеграции, как условие укрепления государственности, институтов гражданского общества, развития социальной инфраструктуры.

Однако следует отчетливо представлять, что участие России в международных системах телекоммуникаций и информационного обмена невозможно без комплексного решения проблем информационной безопасности. Особенно остро проблемы защиты собственных информационных ресурсов в открытых сетях встают перед странами, которые технологически отстают в области информационных и телекоммуникационных технологий от США или Западной Европы. К числу таких стран, к сожалению, относится и Россия. Сегодняшнее состояние российской экономики, неразвитость информационной инфраструктуры, неподготовленность российских пользователей к эффективной работе в открытых сетях не позволяют реализовать полноценное участие страны в таких сетях и пользоваться всеми новыми технологиями.

Запретить разработку и применение информационного оружия, как это сделано, например, для химического или бактериологического оружия, вряд ли возможно. Так же невозможно ограничить усилия многих стран по формированию единого глобального информационного пространства.

Несмотря на то что средства обнаружения атак продолжают развиваться, бороться с угрозами со стороны неконтролируемо растущей сети Internet становится все труднее. Исследование трех миллионов Web-сайтов показало, что 4/5 из них беззащитны. Возрастающая необходимость интеграции корпоративных сетей intranet с Extranet, VPN и удаленным доступом еще больше усложняет задачу противодействия злоумышленникам.

Следует помнить о защите национальных информационных ресурсов и сохранении конфиденциальности информационного обмена по мировым открытым сетям. Вполне вероятно, что на этой почве могут возникать политическая и экономическая конфронтация государств, новые кризисы в международных отношениях. Поэтому информационная безопасность, информационная война и информационное оружие оказались в центре внимания.

Для администратора системы единственный способ обеспечить приемлемый уровень защиты — обладать информацией. Он просто обязан ежедневно просматривать новости в области защиты и пролистывать списки рассылки хотя бы за чашкой кофе.

Пока никто не в состоянии заменить человека по быстроте реакции на информационную атаку, и вложения в обучение и профессиональный рост администраторов защиты информации остаются наиболее эффективным средством противодействия информационным атакам.

Анализ компьютерных преступлений

Если проанализировать статистику компьютерной преступности, то картина получается мрачная.

Урон, наносимый компьютерными преступлениями, сопоставим с доходами от незаконного оборота наркотиков и оружия. Только в США ежегодный ущерб, наносимый «электронными преступниками», составляет около 100 млрд долларов. Высока вероятность того, что в недалеком будущем этот вид преступной деятельности по рентабельности, обороту денежных средств и количеству задействованных в нем людей превысит три вида незаконного бизнеса, которые до недавнего времени занимали первые места по доходности среди незаконной деятельности: торговлю наркотиками, оружием и редкими дикими животными.

Данные социологических исследований деятельности государственных и частных компаний свидетельствуют о том; что уже с первых лет XXI века преступления в экономической сфере будут ориентированы на возможность корыстных экономических действий в информационно-вычислительных комплексах банковских и иных систем.

Количество компьютерных преступлений в кредитно-финансовой сфере постоянно возрастает. Например, онлайновые магазины фиксируют до 25% мошеннических платежных операций. Тем не менее в Западных странах наблюдается активное развитие электронной коммерции — этого сверхрентабельного современного бизнеса. Понятно, что параллельно развитию этой сферы увеличиваются и доходы «виртуальных» мошенников. Последние уже не действуют в одиночку, а работают тщательно подготовленными, хорошо технически и программно вооруженными преступными группами при непосредственном участии самих банковских служащих.

Специалисты в области безопасности отмечают, что доля таких преступлений составляет около 70%.

«Виртуальный» грабитель зарабатывает в несколько раз больше, чем его коллега — обычный налетчик. Кроме этого, исключается перестрелка с охраной и полицией, захват заложников и множество других деяний, не только рискованных для жизни преступника, но и способных значительно увеличить срок его пребывания в тюрьме, конечно, если преступника поймают. Ведь «виртуальные» преступники действуют, не выходя из дома.

Усредненные показатели убытков от хищений с использованием электронных средств доступа только в США превышают 600 тыс. долларов. Это, по меньшей мере, в 6-7 раз больше среднестатистического ущерба от вооруженного ограбления банка.

О том, что сфера электронной коммерции вызывает повышенный интерес в криминальной среде, говорят данные одного из опросов, проведенного в 50 странах мира среди 1600 специалистов в области защиты информации. По итогам опроса выяснилось следующее:

- серверы, связанные с продажей продуктов или услуг через сеть Internet, подвергались нападениям приблизительно на 10% чаще, чем серверы, не используемые для проведения финансовых сделок;
- 22% фирм, занимающихся продажами через Web-серверы, имели потери информации, и только 13% компаний, не продающих продукты через Internet, столкнулись с этой же проблемой;
- 12% респондентов, имеющих электронные магазины, сообщили о краже данных и торговых секретов, и только 3 таких случая зафиксировано у компаний, не продающих продукты через систему Web.

Сумма потерь в результате различного рода мошенничеств в сфере банковских услуг и финансовых операций составила:

- 1989 год — 800 млн долларов;
- 1992 год — 1,2 млрд долларов;
- 1993 год — 1,78 млрд долларов;
- 1997 год — 100 млрд долларов.

Эти показатели продолжают расти, но на самом деле цифры не точные. Реально они могут превышать приведенные данные на порядок. Ведь многие потери не обнаруживаются или о них не сообщают. Поэтому, например, в нашей стране, начиная с 1997 года, ежегодно раскрывается всего лишь 10% компьютерных преступлений.

По данным Национального отделения ФБР по компьютерным преступлениям, от 85% до 97% нападений на корпоративные сети не то что не блокируются, но и не обнаруживаются. Так, например, профинансированные Министерством обороны США испытания показали удивительные результаты. Специальные группы экспертов («tiger team») провели анализ защищенности 8932 военных информационных систем. В 7860 (т. е. 88%) случаях проникновение в «святая святых» было успешным. Администраторы только 390 из этих систем обнаружили атаки и только 19 сообщили о них. Другими словами, в 5% систем были зафиксированы атаки и только в 0,24% случаях от об-

щего числа успешно атакованных систем (или 4,9% от числа зафиксировавших атаки) было заявлено об этом в соответствующие инстанции.

Своеобразная *политика умалчивания* объясняется нежеланием администраторов системы обсуждать с кем-либо подробности несанкционированного доступа в свои сети, чтобы не провоцировать повторения инцидентов и не раскрывать своих методов защиты, которые не всегда бывают действенны.

Так же плохо обстоят дела и в других областях деятельности человека, где используются компьютеры. В отчете «Компьютерная преступность и безопасность. — 1999: проблемы и тенденции», подготовленном Институтом компьютерной безопасности США совместно с отделением Федерального бюро расследования в Сан-Франциско, констатировался резкий рост числа обращений в правоохранительные органы по поводу компьютерных преступлений (32% из числа опрошенных). 30% респондентов сообщили, что их информационные системы были взломаны внешними злоумышленниками. Атакам через Internet подверглись 57% опрошенных, а 55% отметили нарушения безопасности систем со стороны собственных сотрудников. На вопрос «Были ли взломаны ваши Web-серверы и системы электронной коммерции за последние 12 месяцев?» 33% специалистов ответили: «Не знаю».

Наряду с распространением вирусов, всеми специалистами отмечается резкий рост числа внешних атак. Как мы видим, сумма ущерба от компьютерных преступлений неумолимо повышается и было бы не совсем корректно говорить о том, что чаще компьютерные преступления совершаются «виртуальными» мошенниками. Сегодня угроза взлома компьютерных сетей исходит от трех категории лиц (хакеров, кракеров и компьютерных пиратов), каждой из которых присущи свои методы.

Хакеры, в отличие от других компьютерных пиратов,- иногда заранее, как бы бравируя, оповещают владельцев компьютеров о намерениях проникнуть в их системы. О своих успехах они сообщают на сайтах Internet. При этом хакеры, руководствующиеся соревновательными побуждениями, как правило, не наносят ущерба компьютерам, в которые им удалось проникнуть.

Кракеры (cracker) — электронные «взломщики», которые специализируются на взломе программ в корыстных личных целях. Для этого они применяют готовые программы взлома, распространяемые по сети Internet. Вместе с тем, по данным американских экспертов, в последнее время они стали также пытаться проникнуть через Internet в военные и разведывательные компьютерные системы.

Наиболее серьезную угрозу информационной безопасности представляет третий тип: *пираты.* Компьютерные пираты — это высококлассные специалисты фирм и компаний, занимающиеся хищением информации по заказам конкурирующих фирм и даже иностранных спецслужб. Кроме того, ими практикуется изъятие денежных средств с чужих банковских счетов.

Некоторые «специалисты» организуют преступные группы, поскольку рентабельность такого криминального бизнеса очень велика. А это приводит к тому, что ущерб от «виртуальной» преступности в скором времени повысится на порядок (если не больше), чем ущерб от традиционных видов преступного бизнеса. И пока нет эффективных способов нейтрализации этой угрозы.

По выводам представителей компании Symantec, занимающейся вопросами компьютерной безопасности, пользователи, проводящие в Internet пару часов в день,

имеют все шансы подвергнуться атаке хакеров. В течение месяца компания проводила исследования, в которых приняло участие 167 человек, на компьютерах которых были установлены защитные экраны firewall, а специальная программа отслеживала все попытки проникновения в компьютер. Уже при установке firewall выяснилось, что часть компьютеров заражена «троянцами», которых можно использовать для удаленной сетевой атаки или получения конфиденциальной информации с компьютера пользователя. Все участники исследования являлись либо домашними пользователями, либо маленькими компаниями, использующими как dial-up, так и высокоскоростные соединения. На эти компьютеры только за один месяц было совершено 1703 попытки хакерских атак, а внимание хакеров привлекли 159 из 167 участников (95%). В среднем, хакеры предпринимали 56 попыток атак в день, а наиболее излюбленным методом проникновения в чужие компьютеры оказался «троянец» Backdoor.SubSeven. В 68% случаях хакеры пытались установить на чужие компьютеры именно эту программу.

Вирусные атаки

Компьютерные вирусы теперь способны делать то же, что и настоящие вирусы: переходить с одного объекта на другой, изменять способы атаки и мутировать, чтобы проскользнуть мимо выставленных против них защитных кордонов.

Как в повторяющейся каждый год истории, когда эпидемиологическим центрам приходится гадать, от гриппа какой разновидности надо готовить вакцины к середине зимы, так и между появлением новых компьютерных вирусов и их «лечением» поставщиками антивирусных средств проходит время.

Поэтому необходимо знать, что случится, если новый не идентифицированный вирус попадает в вашу сеть, насколько быстро поможет антивирусное решение, скоро ли эта помощь достигнет всех клиентских настольных систем и как не допустить распространения такой заразы.

До широкого распространения Internet-вирусов было относительно немного, и они передавались преимущественно на дискетах. Вирусы достаточно просто было выявить и составить их список после того, как они проявили себя и нанесли вред. Если такой список содержал распознаваемые строки байт (сигнатуры) из программного кода, составляющего вирус, то любой файл (или загрузочный сектор) можно было достаточно быстро просмотреть на предмет наличия такой строки. В случае ее обнаружения файл с большой степенью вероятности содержал вирус.

Большинство пользователей применяют этот метод и до сих пор. Проверка сигнатур вирусов пока является наилучшим способом защиты системы от вирусов.

Конечно, такой подход означает, что кто-то где-то был успешно атакован вирусом, когда вирус был еще неизвестен. Это является серьезной причиной для беспокойства, потому что сегодня вирусы распространяются с электронной почтой, а не через дискеты, а электронная почта — гораздо более быстрое и надежное средство обмена информацией.

Если бы сейчас кто-нибудь «выпустил» такого червя, которого 2 ноября 1988 года сотворил Роберт Тарран Моррис (младший), глобальный финансовый кризис был бы неминуем.

Червь Морриса вывел из строя до 20% компьютеров, подключенных тогда в Internet, что составило около 80 000 компьютеров. Сегодня это число равнялось бы 5 млн и более. Данный вирус «прошелся» по хостам и клиентским машинам. Если бы он был нацелен на маршрутизаторы, то, возможно, поразил бы всю сеть Internet. Ведь каждый выведенный из строя маршрутизатор — это около 100 тыс. остановленных компьютеров. Более того, если из-за червя Морриса прервалось общение относительно немногочисленных университетских групп, исследователей и ученых, то отказ от обслуживания такого же масштаба сегодня привел бы к остановке бизнес-процессов. В результате миллионы людей не смогли бы выполнять свои профессиональные обязанности. В 1988 году на восстановление ушло два дня, сейчас же это потребовало бы значительно больше времени.

Червь использовал изъяны, найденные Моррисом в исходном коде, в том числе незакрытые «дыры» почтовой программы Sendmail, а также утилиты Finger. Он тиражировал себя с такой скоростью, какую не ожидал даже сам Моррис. Поскольку вредоносная программа «вела себя очень деликатно», иными словами, не была запрограммирована на уничтожение данных, у Морриса нашлись сторонники и в сообществе Internet. Сам же Моррис так и не признался, почему запустил червя, ставшего, по существу, первой в Internet атакой на отказ от обслуживания. Ему было тогда 24 года, он отлично разбирался в Unix — операционной системе, которую использовал для создания и запуска вируса.

Тем не менее в 1990 году после судебного разбирательства по иску, поданному правительственными органами, он получил три года условно, штраф в размере 10 тыс. долларов и 400 часов общественных работ.

Эта громкая история привлекла внимание всей мировой общественности. Атака стала катализатором исследований, направленных на повышение защищенности Internet. Уже спустя примерно две недели после этой атаки Министерство обороны связалось с Институтом разработки программного обеспечения (Software Engineering Institute, SEI) Университета Карнеги-Меллона и предложило создать централизованную организацию, которая могла бы ликвидировать аналогичные кризисные ситуации в будущем. В итоге был образован *CERT*.

Как показала эпидемия вируса Melissa в 1999 году, при распространении вирусов с помощью электронной почты тысячи компьютеров могут быть инфицированы за несколько часов, поэтому просто не остается времени на неспешное выяснение, что некий код действительно является вирусом, помещение его в следующий набор сигнатур вирусов и отправку с очередным обновлением антивирусного продукта.

Melissa и ее потомки демонстрируют чрезвычайную точность метафоры: особо вирулентные штаммы склонны к быстрой мутации, благодаря чему они более устойчивы к традиционным противоядиям.

Если бы все вирусы действовали подобно червю Морриса, это было бы не так страшно. Но все больше опасных инфекций оказываются смертельными. Целая колония новых вирусов занимается уничтожением файлов. Например, вирус Explorer.zip немедленно уничтожает все файлы с документами, как только их находит.

Конечно, доля вирусов, намеренно уничтожающих данные, невелика, но общее их число растет отчасти потому, что писать вирусы стало намного проще. Так называемые *макровирусы* легко поддаются изучению и анализу. Для этого злоумышленнику не надо ни шестнадцатеричных редакторов, ни дисассемблеров кода.

Макровирусы представляют собой простые текстовые компоненты обычного офисного настольного приложения, поэтому создание новой разновидности — это всего лишь несколько операций вырезания и вставки (причем обычно новый вирус имеет иную сигнатуру). Вдобавок, традиционные исполняемые вирусы становятся все хитрее: в некоторых из них предусмотрены собственные периодические мутации.

Сейчас по миру «гуляют» более 300 вредоносных программ, представляющих серьезную угрозу компьютерам пользователей. И это лишь малая часть из 50 тыс. вредоносных программных кодов, известных на сегодняшний день.

По словам директора Антивирусного исследовательского центра компании Symantec, они ежедневно получают, в среднем, около 15 новых копий вирусов, хотя большинство из них не реализуются.

Пик активности вирусов обычно приходится на осень и на период после зимних праздников. Именно тогда заканчиваются каникулы в колледжах, во время которых юные программисты получают возможность практиковаться в создании новых вирусов.

Макровирусы, которые инициируются автоматическими задачами внутри таких программ, как Microsoft Word, сегодня представляют серьезнейшую угрозу. Вирусы добрались и до файлов с расширением RTF, ранее считавшиеся не подверженными воздействию вирусов. Существуют также более сложные варианты — *полиморфные* и *скрытые* вирусы, которые мимикрируют, меняя свою внутреннюю структуру.

Помимо вирусов, очень опасны другие типы вредоносного программного обеспечения:

- троянские кони;
- черви;
- враждебные апплеты Java.

Троянский конь, как видно по названию, представляет собой программу, которая на первый взгляд абсолютно безвредна, но имеет скрытую функцию, способную нанести вред компьютеру. Троянский конь обычного типа часто распространяется по электронной почте с целью скопировать пароль доступа компьютера, а затем пересылает украденные данные анонимному получателю.

Черви используют такие компьютерные ресурсы, как память и сетевая полоса пропускания, замедляя работу и компьютеров, и серверов. Кроме того, черви иногда удаляют данные и быстро распространяются по электронной почте.

Враждебные апплеты Java служат для захвата информации или наносят ущерб компьютерам пользователей, которые посещают Web-узлы конкурентов. Пользователь может стать жертвой таких программ, когда щелкает на ссылке, полученной им по электронной почте. Хотя до сих пор враждебные апплеты не наносили серьезного ущерба, именно от них в будущем стоит ждать самых страшных разрушений.

Как уже говорилось, одни вирусы после их написания не используются (но могут), другие же, наоборот, используются очень активно. Хроника вирусного вредительства может быть проиллюстрирована следующими примерами. Так, компания Sophos опубликовала очередной перечень вирусов, наиболее часто встречавшихся в июне 2000 года. Их перечень представлен в табл. 1.1.

Таблица 1.1. Перечень наиболее распространенных в июне 2000 г. вирусов.

VBS/Kakworm	28,5%
VBS/Stages-A	16,9%
VBS/LoveLetter	7,4%
WM97/Melissa	3,2%
W32/Ska-Happy99	2,8%
WM97/Marker-C	2,5%
TroJ/Sub7-21B	2,1%
WM97/Marker-0	2,1%
XM97/Yawn-A	2,1%
WM97/Class-D	2,1%
Прочие	30,3%

Как видно из табл. 1.1, вирус VBS/Kakworm остается наиболее часто встречающимся в мире, хотя Microsoft выпустила патч от него. Данный вирус использует «дыры» в MS Internet Explorer и MS Outlook, что означает возможность заразить компьютер уже при чтении почты, даже не запуская присоединенный файл. Его вредоносность во многом зависит от беззаботности владельцев компьютеров.

Кроме перечисленных, есть еще многие другие вредоносные программы, использующие различные «средства передвижения» и прикрытие. Например, вирус Serbian Badman предназначен для соединения с Web-сервером, загрузки оттуда троянца SubSeven и его инсталляции. Serbian Badman распространяется как эротический видеоклип в файле QuickFlick mpg.exe. Для введения пользователя в заблуждение и скрытия того, что файл исполняемый, в его имени содержатся буквы «mpg» (как для формата MPEG). Кроме того, есть пиктограмма, представляющая видео в этом формате для ОС Windows.

При загрузке данного файла из newsgroup и попытке его визуализации (двойным щелчком) вирус Serbian Badman активизируется, соединяется с сайтом и загружает троянский вирус SubSeven, с помощью которого реализуется удаленное управление зараженными системами. В дополнение к действиям, общим для большинства троянских вирусов, SubSeven может записывать звуки (если зараженный компьютер оборудован микрофоном и звуковой картой), а также производить видеозаписи WebCam и QuickCams. В число других операций входят:

О функции ICQ Spy и регистрации паролей;

- модернизация серверной программы через URL-адрес;
- редактирование Windows Registry;
- изменение конфигурационных установок Windows.

На сегодняшний день не забыты и Internet-черви, подобные написанному Моррисом. Вот лишь некоторые из них.

Червь Jer использует «топорный» метод проникновения в компьютер. На Web-сайт добавляется *скрипт-программа* (тело червя), которая автоматически активизируется

при открытии соответствующей HTML-страницы. Затем выдается предупреждение о том, что на диске создается неизвестный файл. Тонкий расчет сделан на то, что пользователь автоматически ответит **Да,** чтобы отвязаться от назойливой скрипт-программы. Тем самым он пропустит на свой компьютер Internet-червя. Именно таким образом 2 июля 2000 года автор вируса Jer разместил этого червя на одном из сайтов системы Geocities. Заголовок сайта содержал заманчивый текст **THE 40 WAYS WOMEN FAIL IN BED** (40 ВАРИАНТОВ ЗАТАЩИТЬ ЖЕНЩИНУ В ПОСТЕЛЬ). Затем информация об этой странице была анонсирована в нескольких каналах *IRC* (Internet Relay Chat), после чего количество посещений этой страницы превысило 1000 в первый же день. Червь Jer не обладает серьезным деструктивным воздействием. Его код содержит ряд ошибок, из-за которых он распространяется только по каналам IRC, но не по электронной почте. Само появление этого червя свидетельствует о вхождении в моду новой технологии «раскрутки» вирусов в Internet.

Существуют и более опасные экземпляры. Для проведения разрушительных действий в теле червя Dilber, например, интегрированы 5 различных вирусов, среди которых такие опасные экземпляры, как Чернобыль, Freelink и SK. Каждого из них Dilber активизирует в зависимости от текущей даты. Несмотря на столь внушительный разрушительный заряд, данный Internet-червь не представляет большой опасности для пользователей. Из-за незначительной ошибки, допущенной в коде программы, она неспособна к размножению, т. е. рассылке своих копий по электронной почте или по локальной сети.

Internet-червь Scrapworm (VBS/Stages) был выложен злоумышленником на авторском сайте. Через несколько дней этот червь был обнаружен в «диком виде» практически во всех странах мира. Вирус обладает потенциалом обрушить почтовые серверы и, в то же время, не слишком опасно воздействует на инфицированные компьютеры. Червь распространяется, в основном, через электронную почту с помощью MS Outlook, но может использовать и каналы IRC. Причем эта программа рассылает сразу по 100 сообщений. Есть и другие имена этого червя: IRC/Stagesworm, IRC/Stages mi, LIFE_STAGES TXT SHS, ShellScrap Worm, VBS/ LifeStages, VBS/Stages 14558, VBS/ Stages.2542, VBS/Stages worm, VBS_STAGES.

Первый год нового тысячелетия немногим отличается от предыдущего. По Internet вновь гуляет вирус под названием Code Red П. Он представляет собой Internet-червя, распространяющегося через электронную почту. Вирус довольно вредный. Мало того, что, рассылая сам себя, он загружает каналы связи, он еще является троянской программой, позволяющей получить удаленный контроль над зараженным компьютером. Единственное, что может радовать многих пользователей компьютеров: вирус Code Red II может осуществлять свою вредоносную деятельность только на компьютерах с Microsoft IIS, работающих под Windows 2000, то есть на Web-серверах, поэтому навредить офисным и домашним компьютерам он не может. К тому же, уже выпущено «противоядие» от этого вируса.

В настоящее время появился более опасный вирус, распространившийся даже в больших масштабах, чем широко известные LoveLetter и Melissa вместе взятые, — это вирус SirCam. Он поражает в том числе и домашние компьютеры, а также способен отправлять во все концы света не только себя самого, но и произвольные части файлов, находящихся на жестком диске зараженного компьютера. А файлы эти могут быть любые, в том числе и те, которые вы бы не хотели показать посторонним.

Пострадал от компьютерного вируса и отдел ФБР по координированию борьбы с кибератаками. Вирус был получен с электронной почтой и не распознали, хотя на компьютере была установлена последняя версия антивирусной программы. Как только вирус обнаружили, были приняты необходимые меры, однако они не смогли блокировать распространение вируса, попавшего на один из компьютеров отдела и с него распространившегося дальше. Вирус отправился по всем электронным адресам, которые он нашел на зараженном компьютере.

Взлом парольной защиты операционных систем

Проблему безопасности компьютерных сетей не назовешь надуманной. Практика показывает: чем масштабнее сеть и чем ценнее информация, доверяемая подключенным к ней компьютерам, тем больше находится желающих нарушить их нормальное функционирование ради материальной выгоды или просто из праздного любопытства.

В самой крупной компьютерной сети в мире (Internet) атаки на компьютерные системы возникают подобно волнам цунами, сметая все защитные барьеры и оставляя после себя парализованные компьютеры и опустошенные винчестеры. Эти атаки не знают государственных границ. Идет постоянная виртуальная война, в ходе которой организованности системных администраторов противостоит изобретательность компьютерных взломщиков. Наиболее опасным при этом является *взлом парольной защиты операционных систем,* которые содержат системный файл с паролями пользователей сети.

Иногда злоумышленнику удается путем различных ухищрений получить в свое распоряжение файл с именами пользователей и их зашифрованными паролями. И тогда ему на помощь приходят специализированные программы, так называемые *парольные взломщики.*

Криптографические алгоритмы, применяемые для шифрования паролей пользователей в современных операционных системах, в подавляющем большинстве случаев являются слишком стойкими, чтобы можно было надеяться отыскать методы их дешифрования, которые окажутся более эффективными, чем тривиальный перебор возможных вариантов. Поэтому парольные взломщики иногда просто шифруют все пароли с использованием того же самого криптографического алгоритма, который применяется для их засекречивания в атакуемой операционной системе, и сравнивают результаты шифрования с тем, что записано в системном файле, содержащем шифрованные пароли ее пользователей. При этом в качестве вариантов паролей парольные взломщики используют символьные последовательности, автоматически генерируемые из некоторого набора символов.

Данный способ позволяет взломать все пароли, если они содержат только символы из данного набора и известно их представление в зашифрованном виде. Поскольку приходится перебирать очень много комбинаций, число которых растет экспоненциально с увеличением числа символов в исходном наборе, такие атаки парольной защиты операционной системы могут занимать слишком много времени. Однако хорошо известно, что большинство пользователей операционных систем не затрудняют себя выбором стойких паролей (т. е. таких, которые трудно узнать). Поэтому для более эффективного подбора паролей парольные взломщики обычно используют так назы-

ваемые *словари,* представляющие собой заранее сформированный список слов, наиболее часто применяемых на практике в качестве паролей.

Для каждого слова из словаря парольный взломщик использует одно или несколько правил. В соответствии с этими правилами, слово изменяется и порождает дополнительное множество вариантов. Производится попеременное изменение буквенного регистра, в котором набрано слово, порядок следования букв в слове меняется на обратный, в начало и в конец каждого слова приписывается цифра 1, некоторые буквы заменяются на близкие по начертанию цифры (в результате, например, из слова password получается pa55wOrd). Это повышает вероятность точного подбора пароля, поскольку в современных операционных системах, как правило, различаются пароли, набранные заглавными и строчными буквами, а пользователям этих систем настоятельно рекомендуется выбирать пароли, в которых буквы чередуются с цифрами.

Одни парольные взломщики поочередно проверяют каждое слово из словаря, применяя к нему определенный набор правил для генерации дополнительного множества опробуемых паролей. Другие предварительно обрабатывают весь словарь при помощи этих же правил, получая новый словарь большего размера, и затем из него берут проверяемые пароли. Учитывая, что словари обычных разговорных языков состоят всего из нескольких сотен тысяч слов, а скорость шифрования паролей достаточно высока, парольные взломщики, осуществляя поиск со словарем, работают достаточно быстро.

Пользовательский интерфейс подавляющего большинства парольных взломщиков трудно назвать дружественным. После их запуска на экране монитора, как правило, появляется лаконичный запрос **File?,** означающий, что необходимо ввести имя файла, где хранится словарь. Да и документацию к парольным взломщикам обильной не назовешь.

Правда, для этого есть свои объективные причины.

Во-первых, парольные взломщики предназначены исключительно для подбора паролей. Такая узкая специализация не способствует разнообразию их интерфейса и обилию сопроводительной документации.

Во-вторых, авторами большей части парольных взломщиков являются люди компьютерного подполья, которые создают такие программы «на лету» для удовлетворения собственных сиюминутных потребностей, и поэтому редко снабжают их подробной документацией и встроенными справочными системами. Приятное исключение из этого правила составляют только парольные взломщики, созданные специалистами в области компьютерной безопасности для выявления слабостей в парольной защите операционных систем. В этом случае дистрибутив парольного взломщика, помимо самой программы, обязательно включает разнообразные дополнительные сведения, касающиеся технических сторон ее эксплуатации, а также небольшой словарь.

На сегодняшний день в Internet существует несколько депозитариев словарей для парольных взломщиков.

Типовые способы удаленных атак на информацию в сети

Злоумышленники могут предпринимать *удаленные атаки* на компьютерные сети. Строятся такие атаки на основе знаний о протоколах, используемых в сети Internet. В результате успех атаки не зависит от того, какую именно программно-аппаратную платформу использует пользователь. Хотя, с другой стороны, это внушает и известный оптимизм. Кроме того, существуют еще и *внутренние атаки* на информацию в компьютерных сетях (рис. 1.1).

За счет того, что все атаки построены на основе некоторого конечного числа базовых принципов работы сети Internet, становится возможным выделить типовые удаленные атаки и предложить некоторые типовые комплексы мер противодействия им. Эти меры, собственно, и обеспечивают сетевую безопасность (специалисты часто грустно шутят, что сетевая компьютерная безопасность — это «борьба с глупостью пользователей и интеллектом хакеров»).

Таким образом, знание действительно превращается в силу, потому что, во-первых, «кто предупрежден — тот вооружен», а во-вторых, знание разрушает и те мифы и заблуждения, которые сложились у пользователей, и, тем самым, серьезно облегчает работу такой большой структуры, как всемирная сеть Internet.

Наиболее типовыми удаленными атаками на информацию в сети (рис, 1.2) из-за несовершенства Internet-протоколов являются:

- анализ сетевого трафика сети;
- внедрение ложного объекта сети;
- внедрение ложного маршрута.

Рассмотрим характеристики этих удаленных атак. Начнем с анализа сетевого трафика сети.

Для получения доступа к серверу по базовым протоколам *FTP* (File Transfer *Protocol)* и *TELNET* (Протокол виртуального терминала) сети Internet пользователю необходимо пройти на нем процедуру *идентификации* и *аутентификации*. В качестве информации, идентифицирующей пользователя, выступает его *идентификатор* (имя), а для аутентификации используется *пароль*. Особенностью протоколов FTP и TELNET является то, что пароли и идентификаторы пользователей передаются по сети в открытом, незашифрованном виде.

Таким образом, для получения доступа к хостам Internet достаточно знать имя пользователя и его пароль. При обмене информацией два удаленных узла Internet делят информацию, которой обмениваются, на *пакеты*. Пакеты проходят по каналам связи; там пакеты и могут быть перехвачены.

Анализ протоколов FTP и TELNET показывает, что TELNET разбивает пароль на символы и пересылает их по одному, помещая каждый символ пароля в соответствующий пакет, а FTP, напротив, пересылает пароль целиком в одном пакете. Ввиду того, что пароли эти никак не зашифрованы, с помощью специальных программ-сканеров пакетов можно выделить именно те пакеты, которые содержат имя и пароль

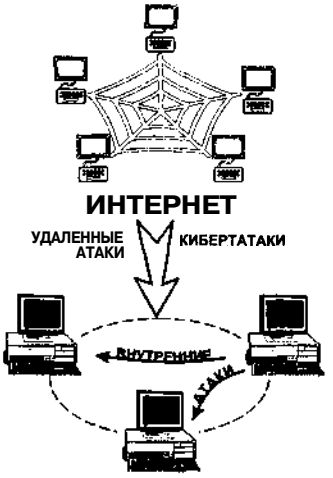


Рис. 1.1. Разновидности атак на информацию в компьютерных сетях

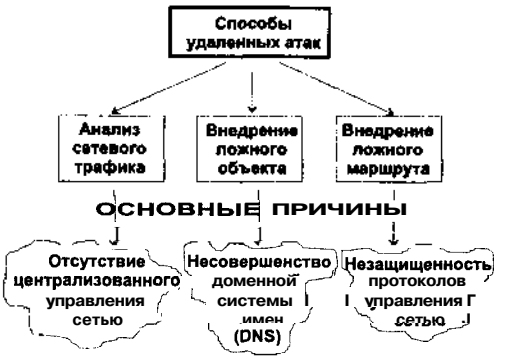


Рис. 1.2. Типовые способы удаленных атак в сети Internet

пользователя. По этой же причине, кстати, ненадежна и столь популярная ныне программа ICQ. Протоколы и форматы хранения и передачи данных обмена ICQ известны. Поэтому трафик ICQ также может быть перехвачен и вскрыт.

Почему все устроено так просто? Проблема заключается в протоколах обмена. Базовые прикладные протоколы семейства TCP/IP были разработаны очень давно — на заре компьютерной техники (в период с конца 60-х до начала 80-х годов) — и с тех пор абсолютно не изменились. В то время основной концепцией построения сети была надежность. Рассматривалась возможность сохранения работоспособности компьютерной сети даже после ядерного удара. За прошедшие годы подход к обеспечению информационной безопасности распределенных сетей существенно изменился. Были разработаны различные протоколы обмена, позволяющие защитить сетевое соединение и зашифровать трафик (например, протоколы SSL, SKIP и т. п.). Однако эти протоколы не сменили устаревшие и не стали стандартом (может быть, за исключением SSL).

Вся проблема состоит вот в чем: чтобы они стали стандартом, к использованию этих протоколов должны перейти все пользователи сети, но так как в Internet отсутствует централизованное управление сетью, то процесс перехода может длиться еще многие годы. А на сегодняшний день подавляющее большинство пользователей используют стандартные протоколы семейства TCP/IP, разработанные более 15 лет назад. В результате, путем простого анализа сетевого трафика (потока информации) возможно вскрыть большинство систем средней защищенности.

Опытные пользователи Internet сталкивались с таким явлением, *как установка защищенного соединения* (обычно при оплате какой-либо покупки в Internet при помощи кредитной карты). Это как раз и есть специальный протокол, который применяет современные криптографические средства с тем, чтобы затруднить перехват и расшифровку сетевого трафика. Однако большая часть сетевого трафика остается по-прежнему незащищенной.

В любой распределенной сети существуют еще такие «узкие места» , как *поиск* и *адресация.* В ходе этих процессов становится возможным внедрение ложного объекта распределенной сети (обычно это ложный хост). Даже если объект имеет право на какой-либо ресурс сети, вполне может оказаться, что этот объект — ложный.

Внедрение ложного объекта приводит к тому, что вся информация, которую вы хотите передать адресату, попадает на самом деле к злоумышленникам. Примерно, это можно представить, как если бы кто-то сумел внедриться к вам в систему, допустим, адресом SMTP (Simple MailTransfer Protocol) — сервера вашего провайдера, которым вы обычно пользуетесь для отправки электронной почты. В этом случае без особых усилий злоумышленник завладел бы вашей электронной корреспонденцией, и вы, даже и не подозревая того, сами переправили бы ему всю свою электронную почту.

Для удобства пользователя в сети, существует несколько уровней представления данных. Каждому из уровней соответствует своя система адресов. Так и на физическом диске файл на одном уровне представления определяется одним лишь своим именем, а на другом — как цепочка адресов кластеров, начиная с адреса первого кластера. При обращении к какому-либо хосту производится специальное преобразование адресов (из IP-адреса выводится физический адрес сетевого адаптера или маршрутизатора сети). В сети Internet для решения этой проблемы используется протокол *ARP* (Address Resolution Protocol).

Протокол ARP позволяет получить взаимно однозначное соответствие IP- и Ethernet-адресов для хостов, находящихся внутри одного сегмента. Это достигается следующим образом: при первом обращении к сетевым ресурсам хост отправляет широковещательный ARP-запрос. Этот запрос получат все станции в данном сегменте сети. Получив запрос, хост внесет запись о запросившем хосте в свою ARP-таблицу, а затем отправит на запросивший хост ARP-ответ, в котором сообщит свой Ethernet-адрес.

Если в данном сегменте такого хоста нет, то произойдет обращение к маршрутизатору, который позволяет обратиться к другим сегментам сети. Если пользователь и злоумышленник находятся в одном сегменте, то становится возможным осуществить перехват APP-запроса и направить ложный ARP-ответ. В итоге обращение будет происходить по физическому адресу сетевого адаптера ложного хоста. Утешением может служить лишь то, что действие этого метода ограничено только одним сегментом сети.

Как известно, для обращения к хостам в сети Internet используются 32-разрядные IP-адреса, уникально идентифицирующие каждый сетевой компьютер. Однако для пользователей применение IP-адресов при обращении к хостам является ре слишком удобным и далеко не самым наглядным. Когда сеть Internet только зарождалась, было принято решение для удобства пользователей присвоить всем компьютерам в сети имена. Применение имен позволяет пользователю лучше ориентироваться в киберпространстве Internet. Пользователю намного проще запомнить, например, имя **www.narod.ru,** чем четырехразрядную цепочку.

Существует система преобразования имен, благодаря которой пользователь в случае отсутствия у него информации о соответствии имен и IP-адресов может получить необходимые сведения от ближайшего *информационно-поискового DNS-сервера* (Domain Name System). Эта система получила название *доменной системы имен* —

DNS. Набирая мнемоническое имя, мы обращаемся тем самым к DNS-серверу, а он уже посылает IP-адрес, по которому и происходит соединение.

Так же, как и в случае с ARP, является возможным внедрение в сеть Internet ложного DNS-сервера путем перехвата DNS-запроса. Это происходит по следующему алгоритму:

1. Ожидание DNS-запроса.
2. Извлечение из полученного запроса необходимых сведений и передача по сети на запросивший хост ложного DNS-ответа от имени (с IP-адреса) настоящего DNS-сервера, в котором указывается IP-адрес ложного DNS-сервера.
3. При получении пакета от хоста изменение в IP- заголовке пакета его IP-адреса на IP-адрес ложного DNS-сервера и передача пакета на сервер (то есть ложный DNS-сервер ведет работу с сервером от своего имени).
4. При получении пакета от сервера изменение в IP-заголовке пакета его IP-адреса на IP-адрес ложного DNS-сервера и передача пакета на хост (хост считает ложный DNS-сервер настоящим).

Современные глобальные сети представляют собой совокупность сегментов сети, связанных между собой через *сетевые узлы.* При этом *маршрутом* называется последовательность узлов сети, по которой данные передаются от источника к приемнику. Для унификации обмена информацией о маршрутах существуют специальные протоколы управления маршрутами; в Internet, например, — это протокол обмена сообщениями о новых маршрутах *ICMP*(Internet Control Message Protocol) и протокол удаленного управления маршрутизаторами *SNMP* (Simple Network Management Protocol). Изменение маршрута — не что иное, как внедрение атакующего ложного хоста. Даже если конечный объект будет истинным, маршрут можно построить таким образом, чтобы информация все равно проходила через ложный хост.

Для изменения маршрута атакующему необходимо послать по сети специальные служебные сообщения, определенные данными протоколами управления сетью, от имени сетевых управляющих устройств (например, маршрутизаторов). В результате успешного изменения маршрута атакующий получит полный контроль над потоком информации, которым обмениваются два объекта распределенной сети, и затем может перехватывать информацию, анализировать, модифицировать ее, а то и просто удалять. То есть становится возможным реализовать угрозы всех типов.

Распределенные атаки на отказ от обслуживания

Атаки на отказ от обслуживания, нацеленные на конкретные Web-узлы, вызывают переполнение последних за счет преднамеренного направления на них Internet-трафика большого объема. Такие атаки, предусматривающие запуск программ, иногда называемых *зомби,* ранее были скрыты на сотнях подключенных к Internet компьютерах, которые принадлежали обычно ничего не подозревающим организациям.

Распределенные атаки на отказ от обслуживания — *DDoS* (Distributed Denial of Service) — сравнительно новая разновидность компьютерных преступлений. Но распространяется она с пугающей скоростью.

Рис. **1.3.** Характеристика средств для атак на отказ от обслуживания

Сетевые атаки на отказ от обслуживания заметно участились после 1996 года, когда на Web-серверы обрушились потоки SYN. Winnuke, teardrop, Land, bonk, snork и smurf — вот лишь некоторые из средств реализации таких атак, которые выводят из строя системы или засоряют сети. Мало того, что сами по себе эти атаки довольно неприятны, теперь они могут инициироваться одновременно с сотен удаленно управляемых атакующих серверов.

На узлах, организованных хакерами, можно найти три инструментальные средства для атак DDoS: trinoo, Tribe FloodNet (TFN) и TFN2K. Совсем недавно появилось еще одно — stacheldraht (что в переводе с немецкого означает «колючие провода»), сочетающее в себе наиболее неприятные качества TFN и trinoo. На рис. 1.3 представлены характеристики средств для атак на отказ от обслуживания.

При обычной сетевой атаке на отказ от обслуживания хакер использует инструментарий для посылки пакетов выбранной им системе. Эти пакеты должны вызвать переполнение и сбой на целевой системе и спровоцировать ее перезагрузку. Довольно часто адрес отправителя таких пакетов искажается, в силу чего обнаружить реальный источник атаки оказывается крайне трудно. Изменить адрес отправителя ничего не стоит, поскольку от жертвы не требуется ответных сообщений.

Организация атаки DDoS по-прежнему под силу одному хакеру, но эффект такой атаки значительно усиливается за счет использования атакующих серверов, известных как *агенты*. Этими агентами, которых в trinoo называют *демонами* (daemon), а в TFN — *серверами* (server), удаленно управляет хакер.

Получить представление о масштабах подобной атаки можно хотя бы на таком примере: в нападении на один сервер университета штата Миннесота в различное время было согласованно задействовано более 1000 систем. Атака не только привела к отключению этого сервера, но и блокировала доступ ко всей сети университета, которую связывали с Internet два соединения.

Прежде чем начать атаку DDoS, хакер должен проделать предварительную работу, в том числе получить доступ с *правами корня* (root) или *администратора* на максимально возможное число систем. До сих пор в качестве агентов при атаке DDoS использовались системы Solaris и Linux. Для получения доступа проводится поиск уязвимых мест систем с помощью таких сканирующих инструментальных средств, как sscan. Затем хакер, используя соответствующий сценарий, проникает в каждую из систем и выполняет установку серверного программного обеспечения.

Для такой инсталляции часто применяется команда удаленного копирования. Сервер, на котором устанавливается программное обеспечение, станет еще одной жертвой взлома, и внезапное увеличение частоты применения команды удаленного копирования обычно служит признаком того, что система не только взломана, но и может использоваться для проникновения на многие другие.

Как только установлен и запущен атакующий сервер — все готово к началу атаки. Чем больше вовлеченных систем, тем массивнее будет атака.

Основными источниками и объектами атак DDoS до сих пор были некоммерческие узлы. Большинство компаний имеют межсетевые экраны, которые помогают предотвратить проникновение на узлы с целью их использования для распределения агентов или в качестве хостов для самих агентов. Однако если межсетевой экран плохо сконфигурирован, это равносильно его отсутствию, поэтому сам факт установки экрана вовсе не гарантирует надежную защиту.

Если атака DDoS началась, остановить ее очень сложно. Пакеты, появляющиеся на вашем межсетевом экране, можно здесь блокировать, но они могут столь же легко переполнить вход вашего Internet-соединения. Если адреса отправителей этих пакетов не были искажены, можно попытаться связаться с задействованными системами и попросить их отключить агентов. Таких систем может быть несколько сотен по всему миру. Если же адреса искажены, вы не узнаете, действительно ли они соответствуют адресам отправителей пакетов до тех пор, пока не разыщете несколько мнимых отправителей (если только выбранные адреса не были адресами RFC 1918).

TFN и trinoo используют различные подходы к удаленному управлению. В обоих случаях хакер применяет клиента для передачи команд, управляющих агентами. Ядро trinoo, называемое *обработчиком,* ждет сигнала, приходящего на порт 27665/TCP для организации соединения, устанавливая его только после того, как передан соответствующий пароль (по умолчанию это betaalmostdone). Как только хакер аутентифицирован обработчиком, он может послать команды всем агентам о начале передачи потоков UDP на одну или несколько целевых систем в течение известного периода времени (от 1 до 2000 с). Адреса отправителя пакетов trinoo не искажаются, в силу чего определить, какие системы являются агентами, довольно просто. Единственная трудность состоит в том, что их может оказаться очень много.

TFN использует ответные сообщения *ICMP* (Internet Control Message Protocol) для взаимодействия с клиентами и агентами. Пакеты того же типа пересылаются и в ответных сообщениях команды Ping. Различным командам присваиваются разные кодовые значения; например, 345 означает старт потока SYN. Инструментарий TFN поддерживает несколько разновидностей атак на отказ от обслуживания: потоки SYN, UDP, ICMP и smurfmg. Поскольку сервер TFN работает как корневой, адреса отправителя могут быть искажены (скорее всего, так и будет сделано), чтобы затруднить поиск источников атаки.

TFN2K появился в декабре 1999 года и предусматривает надежный уровень шифрования (алгоритм CAST-256) при управлении пакетами. Этот метод передачи управляющих сообщений был усовершенствован для того, чтобы разрешить искажение адресов отправителей и передачу пакетов различных типов. Агент TFN2K анализирует сетевой интерфейс и проверяет приходящие из адреса клиентской сети данные, которые он может дешифровать в корректные команды. Все это еще больше усложняет выявление и отслеживание обработчика. Обработчику не передаются никакие ответные сообщения, поэтому он делает вывод, что агент TFN отвечает исключительно по собственному усмотрению.

Инструментарий stacheldraht сочетает в себе возможности TFN и trinoo. Как и TFN, stacheldraht способен искажать адреса отправителей. Кроме того, он может проводить тестирование, чтобы выявить присутствие фильтрации RFC 2267, попытавшись передать пакет с адресом отправителя 3.3.3.3. Если тот блокируется, значит, адреса отправителей по-прежнему искажены, но только в последних восьми битах адреса. Stacheldraht предоставляет возможность модернизации, что позволяет автоматически заменить агентов на новые и запустить их. Stacheldraht использует зашифрованные пакеты TCP (аналогично trinoo) для взаимодействия между клиентами (интерфейс хакера) и обработчиками. Для связи с агентами он также использует зашифрованные пакеты TCP или ICMP. Теперь нетрудно представить себе «удовольствие» стать объектом нападения одновременно сотен хакеров.

Из-за огромного числа систем, вовлеченных в атаки DDoS, попытки прекратить эти атаки практически обречены на провал. Однако существуют превентивные меры, предпринимая которые можно вообще не допустить подобных нападений. Главное — учесть, что атаки начинаются с поиска тысяч уязвимых систем, подключенных к Internet, и последующего проникновения в них. Если эти системы обновить, проникновение можно предотвратить.

Наконец, можно сделать так, чтобы сети не становились источником пакетов с искаженными адресами отправителя. RFC 2267 описывает методику проверки прав доступа, то есть фильтрации пакетов при их входе в сеть так, чтобы только пакеты с легальными адресами отправителя могли преодолеть маршрутизаторы. Остановка всех пакетов с искаженными адресами не предотвратит подобной атаки, но навести порядок после ее завершения будет намного проще.

Методы сбора сведений для вторжения в сеть

Для осуществления несанкционированного доступа в компьютерную сеть требуется, как правило, провести два подготовительных этапа:

- собрать сведения о системе, используя различные методы (рис. 1.4);
- выполнить пробные попытки войти в систему.

Многие владельцы систем часто не представляют, какую кропотливую подготовительную работу должен провести нарушитель, чтобы проникнуть в ту или иную компьютерную систему. Поэтому они самонадеянно полагают: чтобы защитить файл, необходимо только указать для него пароль, и забывают, что любая информация о тех или иных слабых местах системы может помочь злоумышленнику найти лазейку

и обойти пароль, получив доступ к файлу. Таким образом, информация становится легко доступной, если злоумышленник знает, где и что смотреть. Так, даже простая брошюра, описывающая возможности системы, может оказаться весьма полезной хакеру, который не знаком с системой, и может послужить ключом для вхождения в систему.

Следует учитывать, что в зависимости от профессионализма злоумышленника и поставленных им целей возможны различные направления сбора сведений:

- подбор соучастников;
- анализ периодических изданий, ведомственных бюллетеней, документации и распечаток;
- перехват сообщений электронной почты;
- подслушивание разговоров, телексов, телефонов;
- перехват информации и электромагнитного излучения;
- организация краж;
- вымогательство и взятки.

Полная картина вырисовывается в процессе постепенного и тщательного сбора информации. И если начинающие хакеры и прочие злоумышленники должны приложить к этому все свое умение, то профессионалы достигают результатов гораздо быстрее.

Подбор соучастников требует большой и кропотливой работы. Он основан на подслушивании разговоров в барах, фойе отелей, ресторанах, такси, подключении к теле-

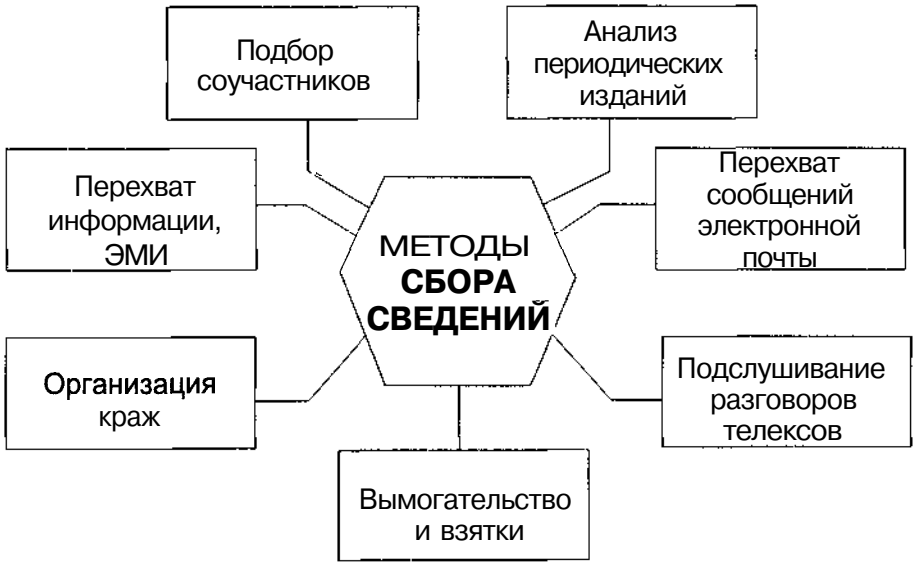


Рис. **1.4.** Методы сбора сведений для НСД в компьютерную сеть

фонам и телексам, изучении содержимого потерянных портфелей и документов. Иного полезную информацию можно извлечь, если предоставляется возможность подсесть к группе программистов, например, в баре. Этот способ часто используют репортеры и профессиональные агенты.

Для установления контактов с целью получить информацию о вычислительной системе или выявить служебные пароли хакеры могут применять разнообразные приемы. Например:

- знакомясь, они представляются менеджерами;
- используют вопросники, раздавая их в фойе фирмы и детально расспрашивая сотрудников о компьютерной системе;
- звонят оператору ЭВМ в обеденное время с просьбой напомнить якобы забытый пароль;
- прогуливаются по зданию, наблюдая за доступом к системе;
- устанавливают контакты с незанятыми в данный момент служащими охраны, которым посетители при входе в здание фирмы должны предъявлять идентификационный код или пароль.

Более злонамеренным, но, возможно, и более успешным, является метод «охоты за мозгами», когда на фирму приходит человек, якобы желающий работать системным программистом или инженером по линиям связи, и просит дать ему консультацию. Удивительно, как много информации может передать простой служащий, не имеющий перспективы роста, но считающий себя достойным более важной и высокооплачиваемой должности, — он может раскрыть коды пользователей, пароли, указать слабые места в сетях связи.

Хакеры могут почерпнуть много полезной информации из газет и других периодических изданий, телевизионных и радиопередач. Это один из наиболее эффективных и наименее рискованных путей получения конфиденциальной информации. Многочисленные фирмы все еще теряют информацию со своих компьютерных систем, ошибочно полагая, во-первых, что она не содержит конфиденциальной информации, и, во-вторых, что все черновые распечатки добросовестно уничтожаются. Именно таким способом хакеры смогли получить весьма полную картину организации компьютерной системы, используя выброшенные распечатки и невостребованные протоколы работы системы, которые сотрудникам вычислительного центра представляются безобидными бумажками.

Перехват сообщений электронной почты производится с помощью компьютера. Обычно для подключения к электронной почте используется бытовой компьютер с модемом, обеспечивающим телефонную связь.

Телефонный канал доступа в такую систему, как правило, незащищен, хотя в последнее время системные операторы требуют установки устройств регистрации пользователей электронной почты. Вплоть до недавнего времени многие справочные системы были оснащены блоками, с помощью которых хакеры могли извлекать большие объемы данных, а также идентификаторы и пароли пользователей.

Недавние аресты и судебные преследования хакеров в США и Великобритании позволили выявить, насколько усложнились способы извлечения информации. Сейчас нет ничего необычного в том, что блоки, установленные хакерами, могут быть зашифрованы, и только отдельные члены преступных группировок могут считывать с них информацию.

Долгое время считалось, что о перехвате сообщений может идти речь лишь в связи с деятельностью военных или секретных служб. Благодаря тому, что число фирм, оснащенных вычислительной техникой, постоянно растет, перехват сообщений стал весьма реальной угрозой и для коммерческого мира. Спектр возможных перехватов весьма широк:

- перехват устных сообщений с использованием радиопередатчиков, микрофонов и микроволновых устройств;
- подслушивание сообщений, передаваемых по телефону, телексу и другим каналам передачи данных;
- контроль за электромагнитным излучением от дисплеев;
- перехват спутниковых или микроволновых передач.

Установкой радиопередатчиков, микрофонов и микроволновых устройств или прослушиванием линий связи обычно занимаются профессиональные хакеры, а также предприимчивые любители и специалисты по системам связи. В последнее время число случаев установки таких устройств возросло. Излюбленными точками бесконтрольного доступа являются телефонные линии.

Существует риск при использовании трехуровневых систем связи, поскольку абонент не в состоянии контролировать работу инженеров, а также доступ в здание и к оборудованию. Передача данных с коммутацией пакетов или с использованием широкополосных линий связи со скоростями в тысячу и миллионы бод вызывает интерес у хакеров. Пакеты могут быть перехвачены, чтобы выкрасть передаваемые сообщения, модифицировать их содержимое, задержать или удалить.

Не следует недооценивать тех трудностей, которые возникают при перехвате больших потоков слабосвязанной между собой информации и при попытках объединить ее в нечто, напоминающее исходное сообщение. Для этого может потребоваться достаточно мощный мини-компьютер, устройство для выделения сигналов отдельных каналов и терминал, на который поступают двоичные цифровые сигналы. Хотя это весьма сложно, но возможно.

Администраторы и менеджеры некоторых фирм имеют возможность брать работу домой или при необходимости связываться и передавать информацию по телефонным каналам в банк данных фирмы. Торговые агенты могут совершать сделки, используя терминалы в номерах отелей, или получать доступ к информации непосредственно из салона автомобиля. Это создает почву для кражи информации непосредственно в домах, автомобилях и отелях с целью вхождения в вычислительную систему.

Преступный мир традиционно играет на таких человеческих слабостях и несчастьях, как чрезмерное увлечение азартными играми, семейные неурядицы, трудноразрешимые финансовые проблемы, долги, оплата медицинских счетов и т. п.

Часто посещая бары, казино, скачки, нанятые хакерами информаторы быстро выявляют людей, готовых идти на контакт. К сожалению, большинство фирм не предусматривает ни штата сотрудников по безопасности, ни каких-либо дисциплинарных процедур, чтобы обнаружить, помешать или снизить риск от действий служащих, попавших под влияние хакеров.

И наконец, получив необходимый объем предварительной информации, компьютерный хакер делает следующий шаг: вторгается в систему. Используемые при этом средства будут зависеть от количества информации, имеющейся в его распоряжении.

Чтобы осуществить несанкционированное вхождение в систему, хакеру требуется знать номер телефона или иметь доступ к линии связи, иметь протоколы работы, описание процедур входа в систему, код пользователя и пароль. Если хакер не знает телефонного адреса порта, он должен либо узнать его, завязывая знакомства, либо воспользоваться автонабирателем.

Итак, мы видим, что действия хакера или иного злоумышленника во многом зависят от его профессионализма и стоящих перед ним задач. Поэтому далее мы рассмотрим общую собирательную модель нарушителя безопасности информации.

Модель нарушителя безопасности информации

Попытка получить несанкционированный доступ к компьютерным сетям с целью ознакомиться с ними, оставить записку, выполнить, уничтожить, изменить или похитить программу или иную информацию квалифицируется как *компьютерное пиратство*. Как социальное явление, подобные действия прослеживаются в последние 10 лет, но при этом наблюдается тенденция к их стремительному росту по мере увеличения числа бытовых компьютеров.

Рост количества компьютерных нарушений ожидается в тех странах, где они широко рекламируются в фильмах и книгах, а дети в процессе игр рано начинают знакомиться с компьютерами. Вместе с тем растет число и серьезных умышленных преступлений. Так, например, известны случаи внедрения в военные системы, нарушения телевизионной спутниковой связи, вывода из строя электронных узлов регистрации на бензоколонках, использующих высокочастотные усилители; известны попытки перевода в Швейцарию сумм около 8,5 млн долларов и разрушения европейской коммуникационной сети связи. Из этого следует, что не только компьютеры, но и другие электронные системы являются объектами злоумышленных действий.

Однако компьютерные преступники не интересуются, насколько хорошо осуществляется в целом контроль в той или иной системе; они ищут единственную лазейку, которая приведет их к желанной цели. Для получения информации они проявляют незаурядную изобретательность, используя психологические факторы, детальное планирование и активные действия. Они совершают преступления, считая, что путь добывания денег с помощью компьютера более легкий, чем ограбление банкой. При этом применяются такие приемы, как взяточничество и вымогательство, о которых заурядный владелец компьютера, возможно, читал, но никогда не предполагал, что сам станет объектом таких действий.

Удивительно мало фирм, где руководство верит в то, что их фирма может пострадать от хакеров, и еще меньше таких, где анализировались возможные угрозы и обеспечивалась защита компьютерных систем. Большинство менеджеров под действием средств массовой информации считают компьютерными нарушителями только школьников и применяют против них такое средство защиты, как пароли. При этом они не осознают более серьезной опасности, исходящей от профессиональных программистов или обиженных руководителей, поскольку не понимают мотивов, которыми руководствуются эти люди при совершении компьютерных пиратств.

Для предотвращения возможных угроз фирмы должны не только обеспечить защиту операционных систем, программного обеспечения и контроль доступа, но и попытаться выявить категории нарушителей и те методы, которые они используют.

В зависимости от мотивов, целей и методов, действия нарушителей безопасности информации можно разделить на четыре категории:

- искатели приключений;
- идейные хакеры;
- хакеры-профессионалы;
- ненадежные (неблагополучные) сотрудники.

Искатель приключений, как правило, молод: очень часто это студент или старшеклассник, и у него редко имеется продуманный план атаки. Он выбирает цель случайным образом и обычно отступает, столкнувшись с трудностями. Найдя дыру в системе безопасности, он старается собрать закрытую информацию, но практически никогда не пытается ее тайно изменить. Своими победами такой искатель приключений делится только со своими близкими друзьями-коллегами.

Идейный хакер — это тот же искатель приключений, но более искусный. Он уже выбирает себе конкретные цели (хосты и ресурсы) на основании своих убеждений. Его излюбленным видом атаки является изменение информационного наполнения Web-

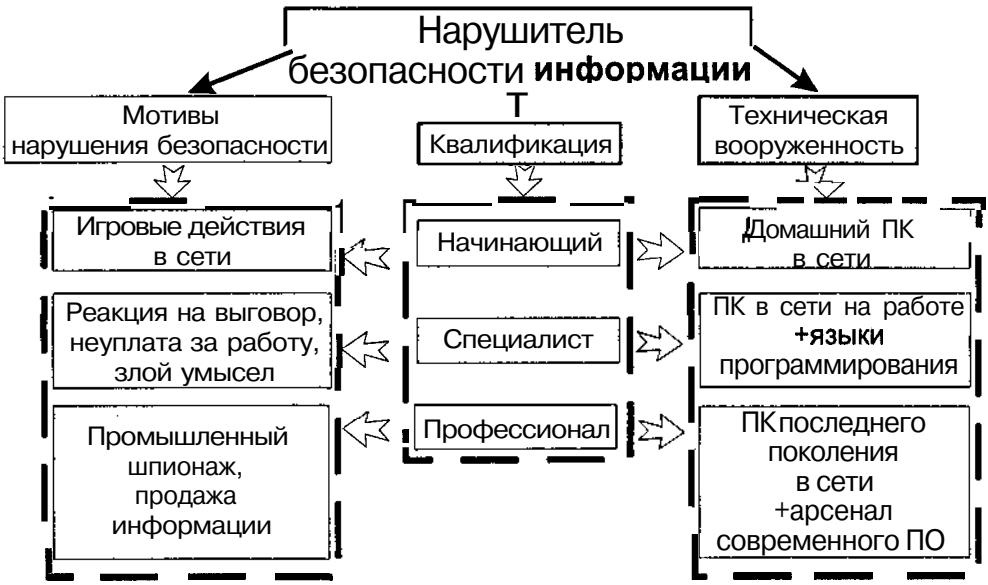


Рис. **1.5.** Модель нарушителя безопасности информации

сервера или, в более редких случаях, блокирование работы атакуемого ресурса. По сравнению с искателем приключений, идейный хакер рассказывает об успешных атаках гораздо более широкой аудитории, обычно размещая информацию на хакерском Web-узле или в конференциях Usenet.

Хакер-профессионал имеет четкий план действий и нацеливается на определенные ресурсы. Его атаки хорошо продуманы и обычно осуществляются в несколько этапов. Сначала он собирает предварительную информацию (тип ОС, предоставляемые сервисы и применяемые меры защиты). Затем он составляет план атаки с учетом собранных данных и подбирает (или даже разрабатывает) соответствующие инструменты. Далее, проведя атаку, он получает закрытую информацию, и наконец, уничтожает все следы своих действий. Такой атакующий профессионал обычно хорошо финансируется и может работать в одиночку или в составе команды профессионалов.

Ненадежный (неблагополучный) сотрудник своими действиями может доставить столько же проблем (бывает и больше), сколько промышленный шпион, к тому же его присутствие обычно сложнее обнаружить. Кроме того, ему приходится преодолевать не внешнюю защиту сети, а только, как правило, менее жесткую внутреннюю. Он не так изощрен в способах атаки, как промышленный шпион, и поэтому чаще допускает ошибки и тем самым может выдать свое присутствие. Однако в этом случае опасность его несанкционированного доступа к корпоративным данным много выше, чем любого другого злоумышленника.

Перечисленные категории нарушителей безопасности информации можно сгруппировать по их квалификации: *начинающий* (искатель приключений), *специалист* (идейный хакер, ненадежный сотрудник), *профессионал* (хакер-профессионал). А если с этими группами сопоставить мотивы нарушения безопасности и техническую оснащенность каждой группы, то можно получить обобщенную модель нарушителя безопасности информации, как это показано на рис. 1.5.

Нарушитель безопасности информации, как правило, являясь специалистом определенной квалификации, пытается узнать все о компьютерных системах и сетях и, в частности, о средствах их защиты. Поэтому модель нарушителя определяет:

- категории лиц, в числе которых может оказаться нарушитель;
- возможные цели нарушителя и их градации по степени важности и опасности;
- предположения о его квалификации;
- оценка его технической вооруженности;
- ограничения и предположения о характере его действий.

Диапазон побудительных мотивов получения доступа к системе довольно широк: от желания испытать эмоциональный подъем при игре с компьютером до ощущения власти над ненавистным менеджером. Занимаются этим не только новички, желающие позабавиться, но и профессиональные программисты. Пароли они добывают либо в результате подбора или догадки, либо путем обмена с другими хакерами.

Часть из них, однако, начинает не только просматривать файлы, но и проявлять интерес именно к их содержимому, а это уже представляет серьезную угрозу, поскольку в данном случае трудно отличить безобидное баловство от злоумышленных действий.

До недавнего времени вызывали беспокойство случаи, когда недовольные руководителем служащие, злоупотребляя своим положением, портили системы, допуская

к ним посторонних или оставляя системы без присмотра в рабочем состоянии. Побудительными мотивами таких действий являются:

- реакция на выговор или замечание со стороны руководителя;
- недовольство тем, что фирма не оплатила сверхурочные часы работы (хотя чаще всего сверхурочная работа возникает из-за неэффективного использования рабочего времени);
- злой умысел в качестве, например, реванша с целью ослабить фирму как конкурента какой-либо вновь создаваемой фирмы.

Недовольный руководителем служащий создает одну из самых больших угроз вычислительным системам коллективного пользования. Это обусловлено еще и тем, что агентства по борьбе с хакерами с большей охотой обслуживают владельцев индивидуальных компьютеров.

Профессиональные хакеры — это компьютерные фанаты, прекрасно знающие вычислительную технику и системы связи. Они затратили массу времени на обдумывание способов проникновения в системы и еще больше, экспериментируя с самими системами. Для вхождения в систему профессионалы чаще всего используют некоторую систематику и эксперименты, а не рассчитывают на удачу или догадку. Их цель — выявить и преодолеть защиту, изучить возможности вычислительной установки и затем удалиться, утвердившись в возможности достижения своей цели.

Благодаря высокой квалификации эти люди понимают, что степень риска мала, так как отсутствуют мотивы разрушения или хищения. Действительно, задержанные и привлекавшиеся к суду нарушители часто упрекали начальство в дурном к ним отношении и оправдывались своей незащищенностью. Некоторые из них предлагали услуги в качестве консультантов фирмам, где накопились подобные проблемы.

Все это свидетельствует о том, насколько опасно наивное отношение к хакерам, которые по-детски стараются продемонстрировать свое умение внедряться в системы, а также показать ошибки и глупость фирм, не имеющих мощных средств защиты. С другой стороны, если их разоблачат, хакеры хотят понести такое наказание, как если бы они не преследовали злого умысла и их действия не носили криминального характера.

Такие личности, когда ими руководят недовольство и гнев, часто отыгрываются на других и относятся к категории людей, которые никогда не настаивают на проведении проверок устройств защиты.

К категории хакеров-профессионалов обычно относят следующих лиц:

- входящих в преступные группировки, преследующие политические цели;
- стремящихся получить информацию в целях промышленного шпионажа;
- хакер или группировки хакеров, стремящихся к наживе.

Приведем некоторые примеры их деятельности.

Заместитель директора одной из фирм, имея доступ к сети информационного обмена, «спускал пары», посылая оскорбительные записки клиентам или перетасовывал телексы. Этими действиями он фактически парализовал работу станции телексной связи.

Другой пример. Злоупотребляя возможностями центральной телексной связи, мошенники смогли похитить 13,8 млн долларов, пересылавшихся телеграфом. В результате прослушивания телефонных разговоров было похищено 780 тыс. ф. ст.

Компьютерные махинации обычно тщательно спланированы и совершаются со знанием дела. Мотивом нарушений, как правило, служат большие деньги, которые можно было получить, практически не рискуя. Вообще профессиональные пираты стремятся свести риск к минимуму. Для этого они привлекают к соучастию работающих или недавно уволившихся с фирмы служащих, поскольку для постороннего риск быть обнаруженным при проникновении в банковские системы весьма велик.

Сложность и высокое быстродействие банковских вычислительных систем, постоянное совершенствование методов ведения и проверки документов, отчетность делают практически невозможным для постороннего лица перехват сообщений или внедрение в систему с целью похищения данных. Существует и дополнительный риск: изменение одного компонента может привести к сбою в работе другого и послужить сигналом к объявлению тревоги.

Чтобы уменьшить риск, хакеры обычно завязывают контакты со служащими, у которых есть финансовые или семейные проблемы. Сотни лет шпионаж используется как метод, вынуждающий людей идти на риск и преступления за минимальное вознаграждение или вовсе без него. Большинство людей могут ни разу в жизни так и не столкнуться с хакером, но бывает, что служащий, не осознавая своих слабостей, например, пристрастия к алкоголю или азартным играм, незаметно для себя становится должником какого-либо букмекера, который, возможно, связан с преступной организацией. Такой служащий может сболтнуть лишнее на какой-нибудь вечеринке, не предполагая, что его собеседник является профессиональным агентом.

Сегодня, когда Internet уже стучится в дверь каждого дома, хакеры становятся настоящим бедствием для государственных и корпоративных компьютерных сетей. Так, по оценкам экспертов США, нападения хакеров на компьютеры и сети федеральных государственных систем происходят в этой стране не реже 50-и раз в день. Во время опроса, проведенного совместно CSI (Computer Security Institute) и ФБР, 68% респондентов ответили, что они в той или иной степени пострадали из-за брешей в системах защиты информации. Многие крупные компании и организации подвергаются атакам несколько раз в неделю, а некоторые даже ежедневно. Исходят такие атаки не всегда извне; 70% попыток злонамеренного проникновения в компьютерные системы имеют источник внутри самой организации.

ГЛАВА 2. ПРОБЛЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

Широкое использование информационных технологий во всех сферах жизни общества делает весьма актуальной проблему защиты информации, ее пользователей, информационных ресурсов и каналов передачи данных от преступных посягательств злоумышленников.

Концентрация информации в компьютерах (аналогично концентрации наличных денег в банках) заставляет одних все более усиливать поиски путей доступа к информации, а других, соответственно, усиливать контроль над ней в целях защиты. Национальная безопасность, юридические вопросы, частная тайна — все это требует усиления внутреннего контроля в правительственных и коммерческих организациях. Работы в этом направлении привели к появлению новой дисциплины — безопасность информации.

Специалист в области безопасности информации отвечает за разработку, реализацию и эксплуатацию системы обеспечения информационной безопасности, направленной на поддержание целостности, пригодности и конфиденциальности данных, накопленных в организации. В его функции входит обеспечение физической (технические средства, линии связи и удаленные компьютеры) и логической (сами данные, прикладные программы, операционная система) защиты информационных ресурсов.

Сложность создания системы защиты информации определяется тем, что данные могут быть похищены из компьютера (скопированы), одновременно оставаясь на месте. Ценность некоторых данных заключается в обладании ими, а не в их уничтожении или изменении.

Обеспечение безопасности информации — дело дорогостоящее, и не столько из-за затрат на закупку или установку различных технических или программных средств, сколько из-за того, что трудно квалифицированно определить границы разумной безопасности и соответствующего поддержания системы в работоспособном состоянии.

Объектами посягательств могут быть как сами материальные технические средства (компьютеры и периферия), так и программное обеспечение и базы данных.

Каждый сбой работы компьютерной сети — это не только моральный ущерб для работников предприятия и сетевых администраторов. По мере развития технологий электронных платежей, «безбумажного» документооборота и серьезный сбой локальных сетей может парализовать работу целых корпораций и банков, что приведет к ощутимым убыткам. Не случайно защита данных в компьютерных сетях становится одной из самых острых проблем.

Обеспечение безопасности информации в компьютерных сетях предполагает создание препятствий для любых несанкционированных попыток хищения или модификации данных, передаваемых в сети. При этом очень важно сохранить такие свойства информации, как:

- доступность;
- целостность;
- конфиденциальность.

Доступность информации — это ее свойство, характеризующее способность обеспечивать своевременный и беспрепятственный доступ пользователей к интересующей их информации.

Целостность информации заключается в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию).

Конфиденциальность — это свойство, указывающее на необходимость введения ограничений доступа к данной информации для определенного круга пользователей.

Следует также отметить, что такие области, как банковские и финансовые институты, информационные сети, системы государственного управления, оборонные и специальные структуры, требуют специальных мер безопасности данных и предъявляют повышенные требования к надежности функционирования информационных систем в соответствии с характером и важностью решаемых ими задач.

Для того чтобы правильно оценить возможный реальный ущерб от потери информации, хранящейся на вашем компьютере или циркулирующей в вашей вычислительной сети, рассмотрим сначала, какие же угрозы при этом могут возникнуть и какие адекватные меры по их защите необходимо принимать.

Проблема безопасности сети для нашей страны является очень важной и актуальной. Однако, в силу относительной новизны информационных технологий, а также того, что Internet, благодаря своей структуре, не требует высокой квалификации пользователей, сложилась довольно опасная ситуация, когда большинство работающих в Internet имеют весьма слабое представление о том, насколько опасной может оказаться эта работа.

Правовые, организационные и технические аспекты информатизации государственных и коммерческих структур находятся в неразрывной связи с обеспечением безопасности информационных ресурсов. Достижение баланса интересов личности, общества и государства в информационной сфере является краеугольным камнем национальных интересов России.

Недавно разразившаяся эпидемия вируса WIN.CIH продемонстрировала, насколько все-таки важной может оказаться информация, хранимая на компьютерах, и сколько неприятностей может доставить внезапная утрата этих данных. О таких вещах обычно не задумываются до тех пор, пока «гром не грянет». Троянская программа Back Orifice делает возможным после своей установки удаленное управление компьютером пользователя, причем пользователь просто не сможет определить, что эта программа установлена.

Актуальность информационной безопасности подтверждает и такой факт, что ежедневно только в компьютерной системе ЦБ РФ фиксируется в среднем 20 атак хакеров и виртуальных грабителей.

Для России проблемы, возникающие в сфере обеспечения информационной безопасности, можно разделить на следующие группы:

- ❑ информационная безопасность на геополитическом уровне;
- О отсутствие органа, координирующего деятельность в сфере информационной безопасности;
- ❑ отсутствие государственной политики в Internet;
- G обеспечение надежных механизмов защиты информации.

Информационная безопасность на геополитическом уровне оставляет желать лучшего. До сих пор не утверждена «Концепция информационной безопасности», которая в настоящее время уже частично устарела. Она ориентирована на применение вероятным противником ядерного и обычного оружия. В ней не учитываются возможности использования современных телекоммуникационных и компьютерных технологий в военных целях.

Стремительное обновление аппаратуры и программного обеспечения (примерно каждые 3 года) влечет за собой необходимость постоянно совершенствовать системы защиты. Для качественной защиты информации в этом случае необходим орган, координирующий деятельность в сфере информационной безопасности в рамках целой страны.

Отсутствие государственной политики в Internet, а именно отсутствие правовых механизмов регулирования всех пользователей во Всемирной паутине — эта проблема актуальна не только для нашей страны, но и для развитых западных стран. Здесь не идет речь о контроле государства над сетью Internet.

Надежные механизмы защиты информации в Internet предотвращают проникновение криминала в сеть, обеспечивают разграничение информации и международное сотрудничество.

Характеристика угроз безопасности информации

Построение эффективной защиты информации в компьютерах и компьютерных сетях невозможно без детального изучения наиболее важных понятий сетевой безопасности.

Еще в недавнем прошлом компьютерами пользовались только крупные организации и исследовательские центры. Доступ к ним имели только немногие специалисты, проверенные соответствующими органами на лояльность. Поэтому проблемы коммерческой или личной безопасности, связанные с утечкой информации, возникали крайне редко. Но в последние годы компьютеры внедряются во все виды деятельности, постоянно наращивается их вычислительная мощность, широко используются компьютерные сети различного масштаба. Все это привело к тому, что угрозы потери конфиденциальной информации стали обычным явлением в компьютерном мире.

Неправомерное искажение, фальсификация, уничтожение или разглашение конфиденциальной информации в любой сети может нанести серьезный, а иногда и непоправимый, материальный или моральный урон многим субъектам в процессе их взаимодействия. В этом случае весьма важным является обеспечение безопасности информации без ущерба для интересов тех, кому она предназначена.

Чтобы обеспечить гарантированную защиту информации в компьютерных системах обработки данных, нужно прежде всего сформулировать цели защиты информации и определить перечень необходимых мер, обеспечивающих защиту. А для этого необходимо в первую очередь рассмотреть и систематизировать все возможные факторы (угрозы), которые могут привести к потере или искажению исходной информации.

Одно из основных базовых понятий — это угроза безопасности компьютерной системы, т. е. потенциально возможное происшествие (преднамеренное или случайное), которое может оказать нежелательное воздействие на саму систему, а также на информацию, хранящуюся в ней.

Иными словами, под угрозой понимается событие (воздействие), которое в случае своей реализации становится причиной нарушения целостности информации, ее потери или замены. Угрозы могут быть как случайными, так и умышленными (преднамеренно создаваемыми).

К случайным угрозам относятся:

О ошибки обслуживающего персонала и пользователей:

О потеря информации, обусловленная неправильным хранением архивных данных;

- ❑ случайное уничтожение или изменение данных;
- ❑ сбои оборудования и электропитания:
- ❑ сбои кабельной системы;
- ❑ перебои электропитания;
- ❑ сбои дисковых систем;
- ❑ сбои систем архивирования данных;
- ❑ сбои работы серверов, рабочих станций, сетевых карт и т. д.
- ❑ некорректная работа программного обеспечения:
- ❑ изменение данных при ошибках в программном обеспечении;
- ❑ заражение системы компьютерными вирусами.
- ❑ несанкционированный доступ:
- ❑ случайное ознакомление с конфиденциальной информацией посторонних лиц.

Необходимо отметить, что зачастую ущерб наносится не из-за чьего-то злого умысла, а просто по причине элементарных ошибок пользователей, которые случайно портят или удаляют данные, жизненно важные для системы. В связи с этим, помимо контроля доступа, необходимым элементом защиты информации в компьютерных сетях является разграничение полномочий пользователей. Кроме того, вероятность ошибок обслуживающего персонала и пользователей сети может быть значительно уменьшена, если их правильно обучать и, кроме того, периодически контролировать их действия со стороны, например, администратора безопасности сети.

Трудно предсказуемыми источниками угроз информации являются аварии и стихийные бедствия. Но и в этих случаях для сохранения информации могут использоваться различные средства.

Наиболее надежное средство предотвращения потерь информации при кратковременном отключении электроэнергии — установка источников бесперебойного питания (UPS). Различные по своим техническим и потребительским характеристикам,

подобные устройства могут обеспечить питание всей локальной сети или отдельного компьютера в течение времени, достаточного для восстановления подачи напряжения или для сохранения информации на магнитных носителях. Большинство UPS выполняют функции еще и стабилизатора напряжения, что является дополнительной защитой от скачков напряжения в сети. Многие современные сетевые устройства (серверы, концентраторы, мосты и др.) оснащены собственными дублированными системами электропитания.

Крупные корпорации и фирмы имеют аварийные электрогенераторы или резервные линии электропитания, которые подключены к разным подстанциям. При выходе из строя одной из них электроснабжение осуществляется с другой подстанции.

Основной, наиболее распространенный, метод защиты информации и оборудования от стихийных бедствий (пожаров, землетрясений, наводнений и т. п.) состоит в создании и хранении архивных копий данных, в том числе, в размещении некоторых сетевых устройств, например, серверов баз данных, в специальных защищенных помещениях, расположенных, как правило, в других зданиях, либо, реже, в другом районе города или в даже другом городе.

Особенностью компьютерной неосторожности является то, что безошибочных программ в принципе не бывает. Если проект практически в любой области техники можно выполнить с огромным запасом надежности, то в области программирования такая надежность весьма условна, а иногда почти не достижима. И это касается не только отдельных программ, но и целого ряда программных продуктов фирм, известных во всем мире.

Как считают эксперты по безопасности, из-за недостатков в программных продуктах Microsoft, связанных с обеспечением безопасности данных в сети Internet, хакеры могут захватывать личные ключи шифров пользователей и действовать от их лица. Поскольку существуют дефекты в некоторых программах Microsoft, включая браузер Internet Explorer и пакет Internet Information Server, ключи шифров можно легко скопировать с жестких дисков компьютеров, подключенных к WWW.

Проблема состоит в том, что форматы файлов, применяемые для защиты личных ключей шифров, до конца не проработаны. Используя лазейки в системе защиты, можно с помощью вирусного программного кода, скрытого на Web-страницах, читать содержимое жестких дисков пользователей во время посещения ими данной страницы. А из-за дефекта в программных интерфейсах криптографии, используемых многими средствами Microsoft, множество ключей могут быть считаны с жесткого диска пользователя по простому запросу. Легкость, с которой это можно выполнить, ставит под угрозу все остальные средства шифрования, применяемые на Web-страницах и в браузерах.

Прорехи в защите популярных сетевых коммутаторов Core Bilder-2500 и CoreBilder-3500 производства 3Com Corp. были обнаружены совсем недавно. Их пользователи неожиданно стали жертвой сетевых злоумышленников. Как оказалось, пользуясь программным обеспечением, которое можно скачать с фирменного узла компании, и работая в режиме отладчика (то есть имея пароль на обслуживание системы), мошенники получали права доступа к содержимому пользовательских каталогов, превосходящие даже полномочия системного администратора. Хакеры получали в свое распоряжение расширенный список команд, пользуясь которыми могли не только читать пользова-

тельские пароли, но и изменять их, что приводило к отключению этих пользователей от сети.

Как считают технические специалисты 3Com, виноваты во всем сервисные службы, которым приходится по экстренным вызовам пользователей, забывших свой пароль, заниматься взломом системы защиты коммутатора. Для дистанционного решения таких проблем службы соответствующих организаций и придумали множество «фирменных» шлюзов для входа в систему с предустановленным паролем.

Компания по расширенной проверке коммутаторов, проведенная специалистами 3Com, показала, что указанный дефект системной защиты в равной мере присущ и коммутаторам CoreBilder серий 6000 и 7000, а также новым выпускам SuperStack-II (Switch-220 и 2700).

Вряд ли найдется хотя бы один пользователь или администратор сети, который бы ни разу не сталкивался с компьютерными вирусами. По данным исследования, проведенного фирмой Creative Strategies Research, 64% из 451 опрошенного специалиста испытали «на себе» действие вирусов. На сегодняшний день дополнительно к тысячам уже известных вирусов появляется 100—150 новых штаммов ежемесячно. Наиболее распространенным методом защиты от вирусов до сих пор остается использование различных антивирусных программ.

Уровень указанных угроз в значительной мере снижается за счет повышения квалификации обслуживающего персонала и пользователей, а также надежности аппаратно-программных и технических средств.

Однако наиболее опасным источником угроз информации являются преднамеренные действия злоумышленников. Спектр их противоправных действий достаточно широк, а итогом их вмешательства в процесс взаимодействия пользователей сети является разглашение, фальсификация, незаконное тиражирование или уничтожение конфиденциальной информации.

Стандартность архитектурных принципов построения оборудования и программ обеспечивает сравнительно легкий доступ профессионала к информации, находящейся в персональном компьютере. Ограничение доступа к ПК путем введения кодов не гарантирует стопроцентную защиту информации.

Включить компьютер и снять код доступа к системе не вызывает особых затруднений: достаточно отключить аккумулятор на материнской плате. На некоторых моделях материнских плат для этого предусмотрен специальный переключатель. Также у каждого изготовителя программы BIOS (AMI, AWARD и др.) есть коды, имеющие приоритет перед любыми пользовательскими, набрав которые можно получить доступ к системе. В крайнем случае можно украсть системный блок компьютера или извлечь жесткий диск и уже в спокойной обстановке получить доступ к необходимой информации.

Угрозы, преднамеренно создаваемые злоумышленником или группой лиц (умышленные угрозы), заслуживают более детального анализа, так как часто носят изощренный характер и приводят к тяжелым последствиям. Поэтому рассмотрим их подробно.

Среди множества угроз безопасности информации проанализируем те, которые связаны с целенаправленным доступом злоумышленников непосредственно к техническим средствам информационно-вычислительных компьютерных сетей и обуслов-

лены недостатками технических и программных средств защиты данных, операционных систем, математического и программного обеспечения.

К умышленным угрозам относятся:

- несанкционированный доступ к информации и сетевым ресурсам;
- раскрытие и модификация данных и программ, их копирование;
- раскрытие, модификация или подмена трафика вычислительной сети;
- разработка и распространение компьютерных вирусов, ввод в программное обеспечение логических бомб;
- кража магнитных носителей и расчетных документов;
- разрушение архивной информации или умышленное ее уничтожение;
- фальсификация сообщений, отказ от факта получения информации или изменение времени ее приема;
- перехват и ознакомление с информацией, передаваемой по каналам связи, и т. п.

Второе базовое понятие — это уязвимость компьютерной системы, т. е. характеристика, которая делает возможным возникновение угрозы. «Все, что может случиться, — случается, что не может случиться, — случается тоже» (известный закон Мэрфи). Согласно этому закону, чем уязвимее система, тем вероятнее успех удаленной атаки на нее.

Собственно атака на компьютерную систему (еще одно базовое понятие) — это поиск и использование злоумышленником уязвимости системы. Другими словами, атака — это реализация угрозы. Второе определение точнее, так как в общем случае система должна быть устойчива как к случайным, так и к преднамеренным враждебным воздействиям. Взаимосвязь базовых понятий угроз безопасности информации приведена на рис. 2.1.

Обычно выделяют три основных вида угроз безопасности: угрозы раскрытия, целостности и отказа в обслуживании (рис. 2.2). Угроза раскрытия заключается в том, что информация становится известной тому, кому не следует ее знать. В терминах компьютерной безопасности угроза раскрытия имеет место всегда, когда получен доступ к некоторой конфиденциальной информации, хранящейся в вычислительной системе или передаваемой от одной системы к другой. Иногда вместо слова «раскрытие» используются термины «кража» или «утечка».

Рис. 2.1. Взаимосвязь базовых понятий угроз безопасности информации

Нарушение конфиденциальности (раскрытие) информации — это не только несанкционированное чтение ваших документов или электронной почты. Прежде всего, это перехват и расшифровка сетевых пакетов (как известно, информация в сети передается пакетами), другими словами, анализ трафика. Обычно с реализацией этой угрозы и начинается большинство серьезных атак. Первая цель взломщиков — выяснение паролей системы. Зная пароли, можно удаленно обращаться к системе без всяких дополнительных ухищрений, войти в нее с ваши-

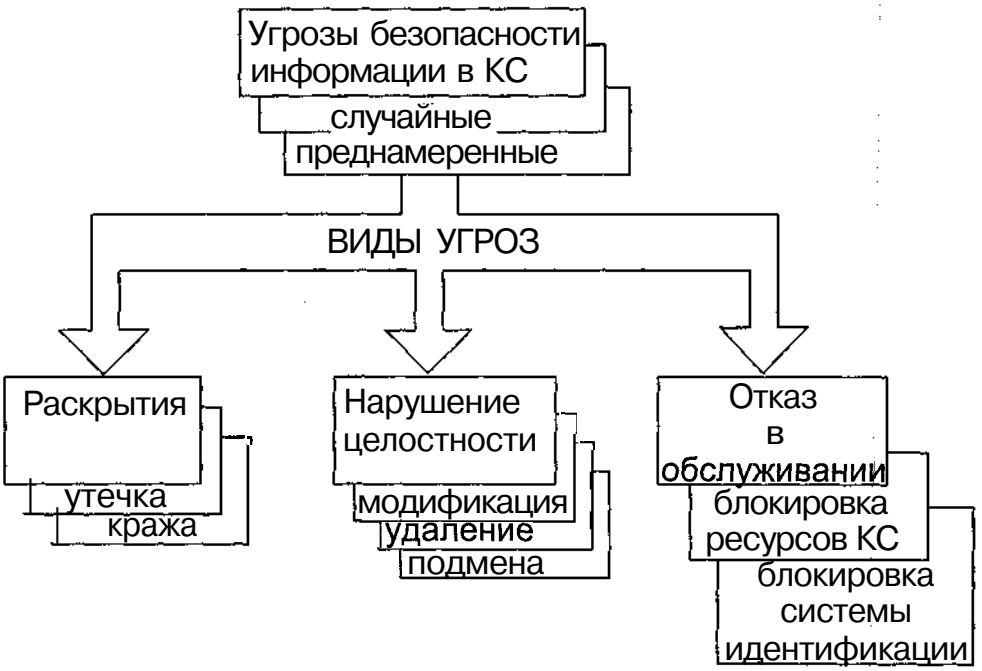


Рис. 2.2. Виды угроз безопасности информации в компьютерных сетях

ми правами и реализовать все остальные угрозы. Поэтому, даже если вы не считаете свою информацию секретной, она все равно нуждается в защите (ведь вы ее храните все-таки в своей системе).

Угроза нарушения целостности включает в себя любое умышленное изменение (модификацию или даже удаление) данных, хранящихся в вычислительной системе или передаваемых из одной системы в другую. Обычно считается, что угрозе раскрытия подвержены в большей степени государственные структуры, а угрозе нарушения целостности — деловые или коммерческие.

Угроза отказа в обслуживании возникает всякий раз, когда в результате некоторых действий блокируется доступ к некоторому ресурсу вычислительной системы.

Реально блокирование может быть постоянным, чтобы запрашиваемый ресурс никогда не был получен, или вызвать только задержку запрашиваемого ресурса, но достаточно долгую для того, чтобы он стал бесполезным. В таких случаях говорят, что ресурс **исчерпан**. Этой угрозой тоже не следует пренебрегать. Если ресурсы любой компьютерной системы всегда ограничены, значит, она имеет «узкое место».

Например, стержнем большинства систем является система разграничения доступа, основанная на введении паролей. В силу того, что распределенная система должна быть доступна, ограничить доступ к системе идентификации нельзя. С другой стороны, система идентификации — ограниченный ресурс. В ходе удаленной атаки он может быть исчерпан (хотя большинство современных систем предусматривают защиту от подобных действий, так как подобная атака хрестоматийна).

Настроив соответствующее программное обеспечение, злоумышленник может запустить механизм множественного ввода паролей (пусть пароли и неверные). Все внешние каналы связи будут забиты ложными паролями. В итоге пользователь, даже имеющий на это право, не сможет войти в систему. Он просто не сможет пробиться к системе идентификации, чтобы ввести правильный пароль. Поэтому большинство современных систем и имеют ограничения на количество неправильно введенных паролей в течение одного сеанса.

Приведем еще пример реализации подобной угрозы: атака серверов электронной почты НАТО во время событий в Югославии. Обладая знаниями лишь об адресах электронной почты (которые общедоступны), **кракеры** просто завалили сервер электронной почты НАТО письмами, содержащими мегабайты информационного мусора.

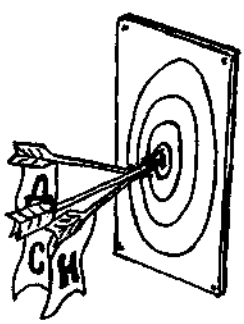
Проблема информационной безопасности постоянно усугубляется процессами проникновения технических средств обработки и передачи данных практически во все сферы и прежде всего в информационно-вычислительные системы. Десятилетие назад, когда компьютеры еще не были объединены в сети, единственной возможностью несанкционированного доступа к информации было знание пароля, который можно было получить от небрежного пользователя или подобрать. Именно несанкционированный доступ к компьютерам и информации, как правило, позволяет реализовать другие виды угроз.

Несанкционированный доступ к информации и его цели

Известно, что, как правило, спецслужбы тщательно следят за каждым своим подопечным, используя все мыслимые контрразведывательные способы: слежку, подслушивание телефонных и всех других разговоров. Возникает закономерный вопрос: какое из этих действий можно рассматривать как получение (способ) несанкционированного доступа.

Способ — это, вообще говоря, порядок и приемы действий, приводящих к достижению какой-либо цели.

Способ несанкционированного доступа (способ НСД) — также совокупность приемов и порядок действий, но с целью получения (добывания) охраняемых сведений незаконным противоправным путем и обеспечения возможности воздействовать на эту информацию (например, подменить, уничтожить и т. п.).



Существующие в настоящее время способы НСД к информации многообразны: применение специальных технических устройств, использование недостатков вычислительных систем и получение секретных сведений о защищаемых данных, как показано на рис. 2.3. Более того, способы НСД связаны с особенностями источников конфиденциальной информации.

Как разнообразны источники, так и способы несанкционированного доступа к ним различны: они зависят от определен-

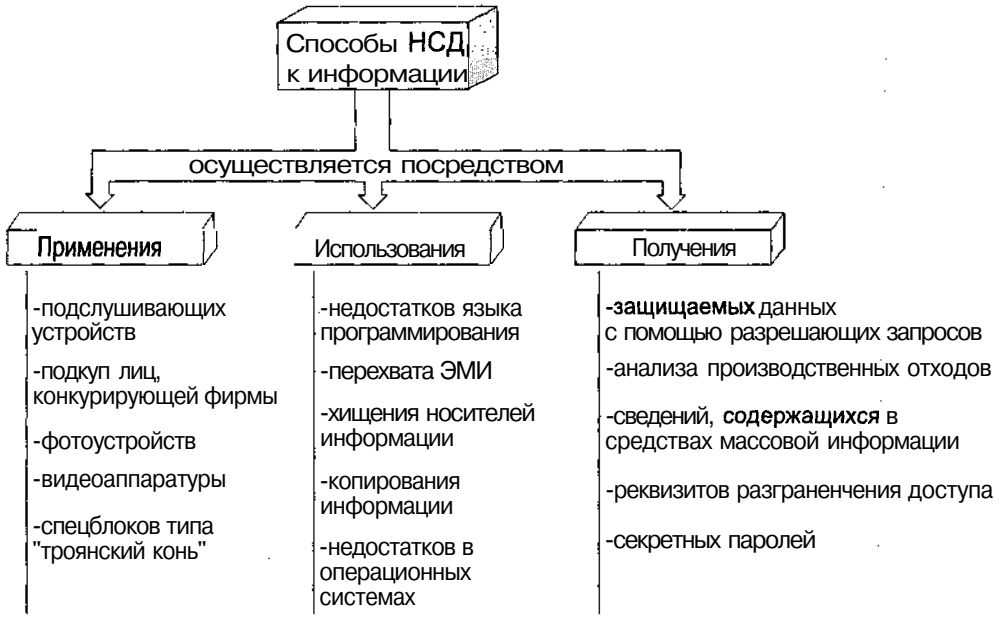


Рис. **2.3.** Способы НСД к конфиденциальной информации

ных условий и ситуаций. Тем не менее, имея формальный набор источников и способов НСД к ним, можно с определенной степенью условности построить формальную модель их взаимосвязи. Такую модель можно было бы назвать обобщенной моделью способов несанкционированного доступа к источникам конфиденциальной информации.

Не вдаваясь в сущность каждого способа, видно, что значительная их часть применима к таким источникам, как люди, технические средства обработки информации и документы. Другие, хотя и реже используемые (в смысле количества источников), никак нельзя отнести к менее опасным. Степень же опасности каждого способа НСД определяется, прежде всего, нанесенным ущербом.

Зададим вопрос: «А какие же цели преследует злоумышленник, осуществляя несанкционированный доступ к источникам конфиденциальной информации?». Попробуем ответить на него подробно.

Во Введении уже было кратко сказано о проблемах, связанных не только с обеспечением сохранности предпринимательской информации (как вида интеллектуальной собственности), но и безопасностью юридических и физических лиц, охраной их собственности. Поскольку информация имеет цену, то уже сам факт получения информации злоумышленником приносит ему определенный доход, таким способом ослабляя возможности конкурента. Отсюда главная цель — получение информации о составе, состоянии и деятельности объекта конфиденциальных интересов для удовлетворения своих информационных потребностей.

Другая корыстная цель — изменение информации, циркулирующей на объекте конфиденциальных интересов. Такое действие может привести к дезинформации по опре-

деленным сферам деятельности, учетным данным, результатам решения некоторых задач. Вместе с тем следует отметить, что трудно вносить изменения или осуществлять дезинформацию. Чтобы выдать ложную информацию за истинную, необходимо предусмотреть комплекс специальных мероприятий, согласованных с общим ходом событий по времени, месту, цели и содержанию, а это требует глубокого знания информационной обстановки на объекте и в регионе. Отдельные ложные сведения не всегда могут дать положительный эффект. Кроме того, они просто могут раскрыть намерения злоумышленника провести модификацию или дезинформацию.

Самая опасная цель — уничтожение накопленных информационных массивов в документальной или магнитной форме и программных продуктов. Уничтожение — это противоправное действие, направленное на нанесение материального и информационного ущерба конкуренту со стороны злоумышленника.

Таким образом, злоумышленник преследует три цели:

- получить необходимую информацию в требуемом для конкурентной борьбы объеме и ассортименте;
- иметь возможность вносить изменения в информационные потоки конкурента в соответствии со своими интересами;
- нанести ущерб конкуренту путем уничтожения материала информационных ценностей.

Полный объем сведений о деятельности конкурента не может быть получен только каким-нибудь одним из возможных способ доступа к информации. Чем большим объемом информации обладает злоумышленник, тем больших успехов он может добиться в конкурентной борьбе. На успех может рассчитывать тот, кто быстрее соберет необходимую информацию (причем, как можно больше), обработает ее и примет правильное решение.

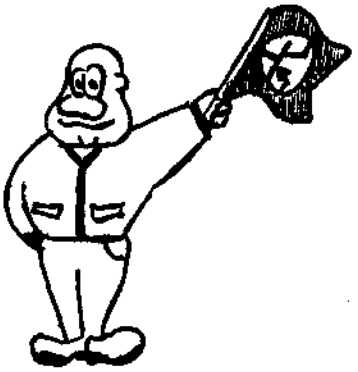
От целей зависит как выбор способов действий, так и количественный и качественный состав привлекаемых сил и средств посягательства на чужие секреты. Все перечисленные цели подразумевают получение доступа к определенной информации. За исключением обработки информации, получаемой из открытых источников, доступ этот носит негласный, а следовательно, несанкционированный характер. Поэтому рассмотрим сначала, как осуществляется НСД к информации.

Способы НСД к информации через технические средства

На современном этапе развития общества уже явно не достаточно использования компьютера автономно от других, поэтому их объединяют в компьютерные сети для обмена информацией, используя различные каналы связи и, следовательно, различные технические средства.

Каждая электронная система, содержащая в себе совокупность элементов, узлов и проводников, обладает источниками информационного сигнала и, естественно, каналами утечки конфиденциальной информации.

Утечка информации через технические средства может происходить, например, за счет:



О микрофонного эффекта элементов электронных схем;

- ❑ магнитной составляющей поля электронных схем и уст ройств различного назначения и исполнения;
- ❑ электромагнитного излучения низкой и высокой частоты;
- ❑ возникновения паразитной генерации усилителей различного назначения;
- ❑ наводок по цепям питания электронных систем;
- ❑ наводок по цепям заземления электронных систем;
- ❑ взаимного влияния проводов и линий связи;
- ❑ высокочастотного навязывания мощных радиоэлектронных средств и систем;

О подключения к волоконно-оптическим системам связи.

Каждый из этих каналов будет иметь структуру в зависимости от условий расположения и исполнения.

Каналы утечки информации и способы несанкционированного доступа к источникам конфиденциальной информации объективно взаимосвязаны. Каждому каналу соответствует определенный способ НСД.

Вариант взаимосвязи способов несанкционированного доступа к объектам и источникам охраняемой информации и каналов утечки конфиденциальной информации приведен в табл. 2.1.

Таблица 2.1. Взаимосвязь способов НСД и каналов утечки информации.

Способ несанкционированного доступа	Тип канала утечки информации			
	Визуальный	Акустический	Электромагнитный (магнитный, электрический)	Материально-вещественные
Подслушивание		+	+	
Визуальное наблюдение	+			
Хищение			+	+
Копирование			+	+
Подделка			+	+
Незаконное подключение		+	+	
Перехват		+	+	
Фотографирование	+			
Итого по виду канала	2	3	6	3

Как видим, наиболее опасными являются электромагнитные каналы утечки информации.

Имея современные технические средства, любая информационная система может оперативно и в полном объеме удовлетворять информационные потребности пользователей. Чем больше средств, тем успешнее работает система. Однако любые технические средства по своей природе потенциально обладают техническими каналами утечки информации. Это расширяет возможности не только в плане использования их конкурентами в криминальных интересах, но и предоставляет дополнительные воз-

можности по несанкционированному доступу к источникам конфиденциальной информации через технические средства информационных систем.

Наличие каждого источника образования канала утечки информации и его конкретные характеристики изучаются, исследуются и определяются конкретно для каждого образца технических средств на оборудованных для этого испытательных стендах в специальных лабораториях.

Противоправные действия злоумышленников, направленные на добывание информации, реализуются пассивными и активными способами.

К пассивным можно отнести использование технических каналов утечки информации без непосредственного контакта или подключения к источнику информации. Эти способы ориентированы, как правило, только на получение информации.

К активным относятся такие способы НСД, как незаконное подключение к каналам, проводам и линиям связи, высокочастотное навязывание, установка в технические средства микрофонных и телефонных радиозакладок, а также несанкционированный доступ к информации, отрабатываемой на ПК, ее копирование, модификация, хищение, визуальное наблюдение экранов и т. д.

Поскольку в настоящее время достижения современных технологий позволяют передавать информацию практически на любые расстояния и представлять данную информацию в любом виде (буквенно-цифровом, речевом, графическом и т. п.), в том числе в виде электронной почты, факса, телетекста, видеотекста, телеметрики, увеличивается и число потенциально возможных каналов утечки информации при неправильном использовании линий связи.

Рассмотрим основные способы несанкционированного доступа к конфиденциальной информации через технические средства. Для передачи информации используют различного вида каналы связи.

Каналы связи, по которым передается компьютерная информация, подразделяются на:

- проводные;
- волоконно-оптические;
- беспроводные (радиотехнические).

Способы НСД к проводным линиям связи

Наиболее часто для передачи информации применяются телефонные линии в качестве проводных линий связи. Это связано с тем, что большинство компьютеров используют для передачи данных модемы, подключенные к телефонной линии.

Способы, которыми может вестись прослушивание телефонных линий, и какая при этом используется аппаратура, представлены на рис. 2.4.

Рассмотрим кратко эти способы. Укажем общепринятые способы подслушивания линии, связывающей компьютеры:

- непосредственное подключение к телефонной линии:
  - контактное — последовательное или параллельное (прямо на АТС или где-нибудь на линии между телефонным аппаратом и АТС);
  - бесконтактное (индукционное) подключение к телефонной линии;
  - помещение радиоретранслятора («жучка») на телефонной линии:

- последовательное включение;
- параллельное включение.

Непосредственное подключение к телефонной линии — наиболее простой и надежный способ получения информации. Такое подключение осуществляется на телефонной станции либо на любом участке линии от потребителя до АТС.

Чтобы обнаружить нужные провода, подсоединяют переносную телефон-трубку к любой паре промежуточных контактов и набирают номер объекта. Проведя кончиками пальцев, монеткой, неоновой лампой или светодиодным пробником по отдельным клеммам, регистрируют (через удар током, сильное искрение, вспыхивание светодиода) явно повышенное (до 100 В и более) напряжение. Отыскав подобным образом требуемую линию, от нее пробрасывают к близлежащему посту прослушивания либо установленному невдалеке магнитофону неприметную отводку, причем в качестве последней можно задействовать всегда имеющиеся в кабеле неиспользованные провода.

Так как АТС переключает линию на разговор при шунтировании ее сопротивлением порядка 1000 Ом, применение для подслушивания аппаратуры с низкоомным входом вызывает перегрузку телефонной сети и падение напряжения, причем высока вероятность обнаружения подключения. Поэтому параллельное подключение к линии стараются производить через сопротивление номиналом в 600-1000 Ом.

Контактное подключение — самый простой способ незаконного подключения, например, параллельного телефонного аппарата или модема. Более совершенным является подключение к линии связи с помощью специальных согласующих устройств типа согласующих трансформаторов или интерфейсных плат персональных компьютеров.

Наиболее часто используется способ физического подключения к линии телекоммуникации, осуществляемого через Y-образный кабель, один разъем которого подключен к интерфейсной карте средства злоумышленника, а два других устанавливаются в разрыв контролируемой линии. При таком способе включения сохраняется прямое электрическое соединение аппаратуры канала передачи данных и оконечного оборудования. В этом случае компьютер злоумышленника является полностью пассивным устройством.

Бесконтактное подключение к линии связи осуществляется двумя путями:

- за счет электромагнитных наводок на параллельно проложенные провода рамки;
- с помощью сосредоточенной индуктивности, охватывающей контролируемую линию.

В обоих случаях подслушивание реализуется за счет использования явления электромагнитной индукции. Индукционное подсоединение к телефонной линии позволяет уклониться от непосредственного контакта с телефонной сетью, поэтому его довольно трудно обнаружить.

Принцип действия такой отводки строится на том, что вокруг обычных проводов при проходе по ним электрического тока возникает электромагнитное поле, наводящее индукционный ток в расположенном поблизости проводнике. Для реализации этого эффекта один из проводов наружной линии обматывают вокруг миниатюрной много-

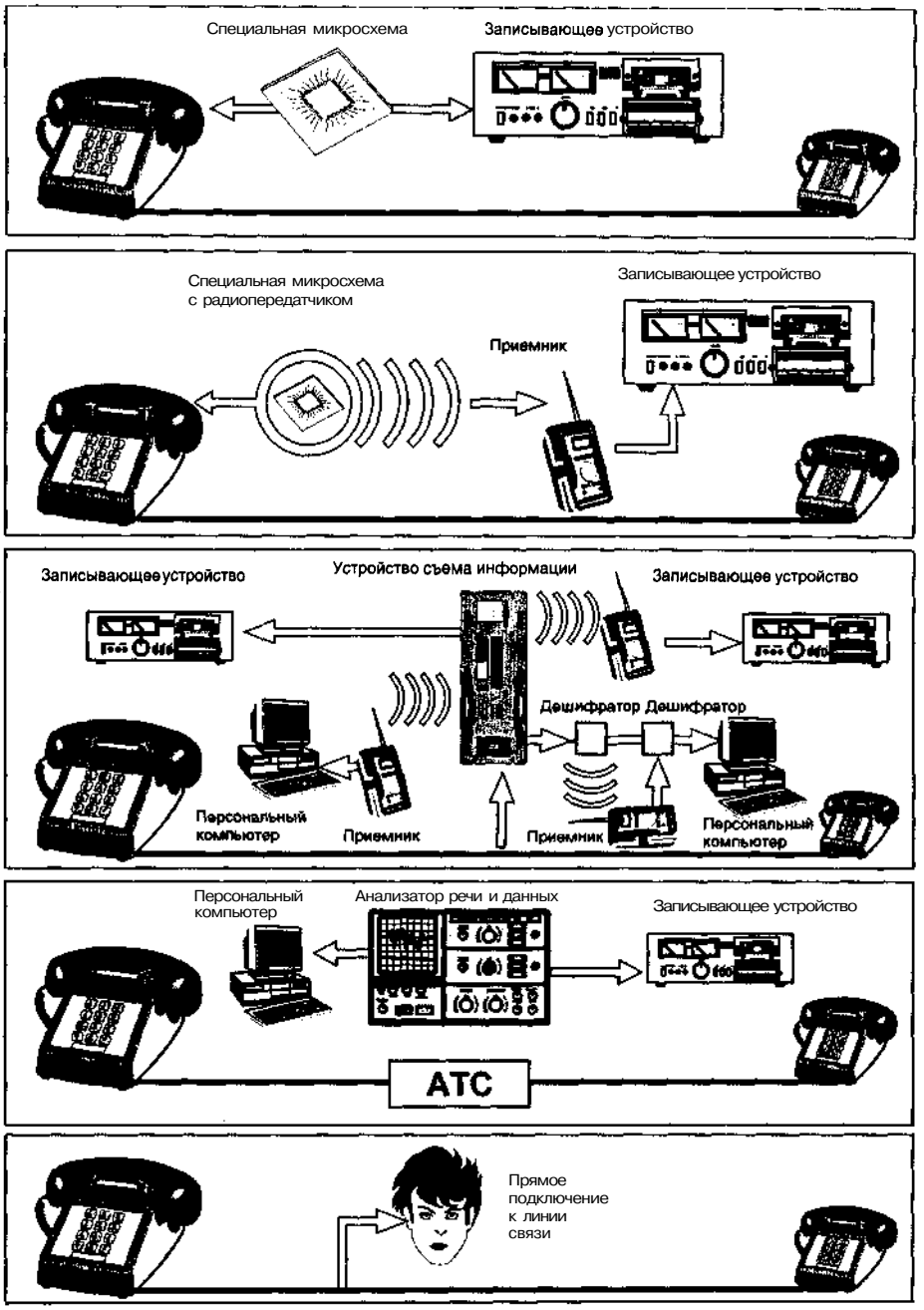


Рис. 2.4. Способы прослушивания проводных линий связи

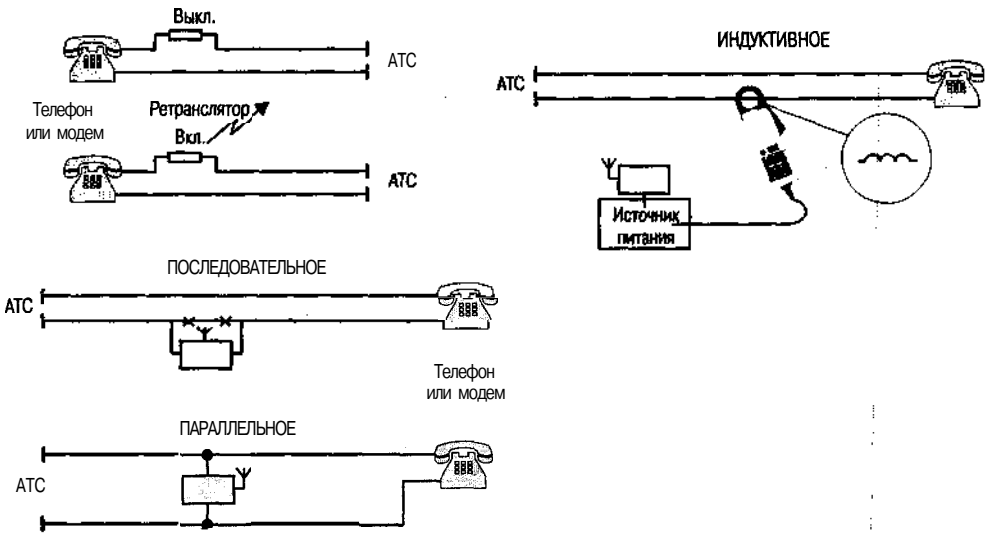


Рис. 2.5. Способы подключения радиоретрансляторов

витковой катушки с ферромагнитным сердечником либо размещают его вблизи подобной же катушки в броневом сердечнике. Выводы импровизированного трансформатора подсоединяют к усилителю низкой частоты, диктофону или микропередатчику. Недостатки подобного приема — невысокий уровень засекаемого сигнала, поэтому обычно требуется его дополнительное усиление, а также явная склонность такого датчика реагировать на посторонние электромагнитные колебания.

Качество принимаемого сигнала определяется подбором характеристик индукционного датчика, усилением и настройкой усилителя низкой частоты. Полоса пропускания обязательно должна быть регулируемой. Это позволяет отфильтровать другие сигналы наводок и помех и выделить именно интересующий сигнал.

Радиопередатчик (радиомикрофон, радиоретранслятор), подключенный к телефонной линии, часто используют, когда применение демаскирующих отводок вызывает некоторые затруднения. Он превосходно ретранслирует циркулирующую информацию туда, где установлен приемник. Различают два способа такого подключения: последовательное и параллельное (рис. 2.5).

В первом случае миниатюрный передатчик включают в разрыв линии и питают его от линии только в момент разговора. Таким образом, ретранслятор действует неограниченно долго, однако напряжение в телефонной сети несколько снижается, что может привести к обнаружению ретранслятора.

Во втором стандартном варианте передатчик подсоединяют параллельно линии и обеспечивают, в зависимости от тока потребления, питанием от линии или от автономного источника питания. Данный образец сложнее обнаружить (происходит бросок напряжения в линии только в момент подсоединения), но период его автономной работы может ограничиваться емкостью применяемых батарей (которая, впрочем, тратится лишь в периоды использования телефона). В конструктивном исполнении все

эти устройства представляют собой маломощные, преимущественно транзисторные генераторы ультракоротких волн (27-900 МГц), несущие которых модулированы перепадами напряжения или тока, возникающими в линии при телефонном разговоре.

Существуют системы прослушивания телефонных разговоров, не требующие непосредственного электронного соединения с телефонной линией. Эти системы используют индуктивный способ (при помощи катушек) съема информации. Они достаточно громоздки, так как содержат несколько каскадов усиления слабого НЧ-сигнала и обязательный внешний источник питания. Поэтому такие системы не нашли широкого применения на практике.

Для приема информации от телефонных радиоретрансляторов используются такие же приемники, как в акустических устройствах съема информации по радиоканалу.

В настоящее время появились системы перехвата факсовой и модемной связи, которые при использовании персонального компьютера со специальным программным обеспечением позволяют расшифровать информацию.

Способы НСД к волоконно-оптическим линиям связи

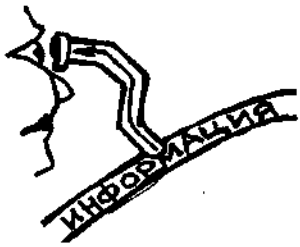
В наше время наиболее эффективной и перспективной передающей средой является волоконно-оптический кабель, с помощью которого образуются волоконно-оптические системы передачи информации, получившие в настоящее время широкое распространение. Информация по такому кабелю передается в виде пульсирующего светового потока, на который практически не влияют электрические и магнитные помехи. Кроме того, трудность перехвата информации, проходящей по волоконно-оптическому кабелю, повышает безопасность связи. Такой кабель обеспечивает передачу данных на большие расстояния со скоростью до десятков гигабит в секунду и используется, в основном, в протяженных магистральных линиях связи. Оптоволокно применяется и для построения компьютерных сетей с высокой пропускной способностью.

В отличие от металлических кабелей связи, в которых переносчиком информации является электрический ток, в оптоволокне этим целям служит поток фотонов в диэлектрике высокой прозрачности (в сверхчистом кварце или полимерных материалах). Они являются хорошими диэлектриками, вследствие чего оптические волокна, а значит, и оптоволоконные кабели не чувствительны к электромагнитным помехам. Кроме того, они значительно устойчивее к различным агрессивным химическим средам, чем металлические кабели.

При равных диаметрах оптические кабели имеют большее, чем кабели других видов, количество информационно-проводящих жил, так как диаметр световодов вместе с защитной оболочкой составляет не более 250 мкм. Благодаря малому затуханию световой энергии в световоде и незначительному искажению формы сигналов оптоволоконные кабели могут быть намного большей длины, чем металлические.

Несанкционированное подключение возможно и к волоконно-оптическим линиям связи. Задача эта не простая, но, как и в рассмотренных выше случаях, возможно контактное и бесконтактное подключение.

Для контактного подключения удаляют защитные слои кабеля, стравливают светоотражающую оболочку и изгибают оптический кабель под углом, необходимым для снятия информации. При таком подключении к волоконно-оптической линии связи



обнаружить утечку информации за счет ослабления мощности излучения бывает очень трудно. Это связано с тем, что чувствительность существующих приемных устройств в процессе несанкционированного доступа обеспечивает съем необходимой информации при отборе всего 0,001% передаваемой мощности, а дополнительные потери при изгибе кабеля находятся в пределах 0,01-1,0 дБ в зависимости от угла изгиба кабеля.

Для бесконтактного подключения в волоконно-оптическую линию связи в качестве элемента съема светового сигнала используется стеклянная трубка, заполненная жидкостью с высоким показателем преломления и с изогнутым концом, жестко фиксированная на оптическом кабеле, с которого предварительно снята экранная оболочка. На отогнутом конце трубки устанавливается объектив, фокусирующий световой поток на фотодиод, уже с которого электрические сигналы поступают на усилитель сигналов, усиливающий их до необходимого уровня.

Способы НСД к беспроводным линиям связи

В настоящее время электронные средства коммуникации получили повсеместное распространение, что позволяет получать массу всевозможной информации об исследуемом объекте. Так уж устроен мир, что любое техническое изобретение, расширяющее наши возможности и создающее для нас дополнительный комфорт, неизбежно имеет и отрицательные стороны, которые могут представлять потенциальную опасность.

Передача информации с помощью высокочастотных радиоволн, которые также относятся к передающей среде, позволяет в УКВ и СВЧ диапазонах обеспечить очень много линий связи для компьютерных сетей там, где прокладка обычных кабелей — затруднительное дело.

В беспроводных линиях связи соединения осуществляются со скоростью от 256 кбит/с до 2 Мбит/с. Возможность влияния помех на радиоканал и большая вероятность перехвата информации снижают надежность данной передающей среды. Однако при использовании новейших западных и российских технологий, в частности, при переходе к сотовой системе с применением стандарта CDMA, появилась возможность строить радиосети в масштабе города и даже развертывать глобальные системы передачи информации.

Перехват электромагнитных излучений основан на широком использовании самых разнообразных радиоприемных средств, средств анализа и регистрации информации, а также таких, как антенные системы, широкополосные антенные усилители, панорамные анализаторы, промежуточная и оконечная аппаратура и др.

Следует отметить, что, по сравнению с другими способами добывания конфиденциальной информации, перехват информации, передаваемой по радиоканалу, обладает следующими особенностями:

- информацию можно получить без непосредственного контакта с источником;
- на прием сигналов не влияет ни время года, ни время суток;
- прием информации происходит в реальном масштабе времени, в момент ее передачи или излучения;

- реализуется скрытно, источник информации зачастую и не подозревают, что его подслушивают;
- дальность перехвата ограничена только особенностями распространения радиоволн соответствующих диапазонов.

При использовании компьютерных сетей используются различные варианты беспроводного радиодоступа. Рассмотрим некоторые из них.

Технология беспроводной связи Bluetooth

Bluetooth — это современная технология беспроводной связи, разработанная для передачи сигнала на небольшие расстояния, которая используется при подключении к компьютеру различных мобильных устройств.

Bluetooth — конкурент таким технологиям, как IEEE 802.11, HomeRF и IrDA, хотя последняя и не предназначена для построения локальных сетей, но является самой распространенной технологией беспроводного соединения компьютеров и периферийных устройств.

В отличие от технологии инфракрасной связи IrDA (Infrared Direct Access), работающей по принципу «точка-точка» в зоне прямой видимости, технология Bluetooth была создана для работы по принципу «точка-точка» и по принципу многоточечного радиоканала для офисного применения (рис. 2.6), управляемого многоуровневым протоколом, похожим на протокол мобильной сотовой связи GSM.

Основными преимуществами этой технологии можно считать следующие:

- многоточечность, то есть в сети могут присутствовать не 2 устройства, как в случае IrDA, а несколько;
- не требуется прямой видимости (используются нелицензируемые частоты порядка 2,44 ГГц);
- дальность от 10 м в текущих реализациях до нескольких десятков метров в перспективе (против 1—2 м для IrDA).

Основной идеей новой технологии является предоставление возможности легкого и удобного беспроводного соединения различных устройств, а также организации беспроводной локальной сети.

Применяя данную технологию, пользователь может организовывать обмен информацией голосом между всевозможными устройствами (например настольным компьютером, переносным компьютером и сотовым телефоном). То есть, скажем, приходите вы в офис, а ваш переносной компьютер тут же автоматически синхронизирует адресную книгу и календарь с настольным компьютером и передает новые контакты на ваш мобильный телефон.

В перспективе, технология позволяет объединять любые электронные устройства, вплоть до холодильников, стиральных машин, микроволновых печей и дверных замков (только представьте: ваш холодильник передает на ваш сотовый, что в нем закончилось молоко, а тот, в свою очередь, отправляет вашему компьютери-

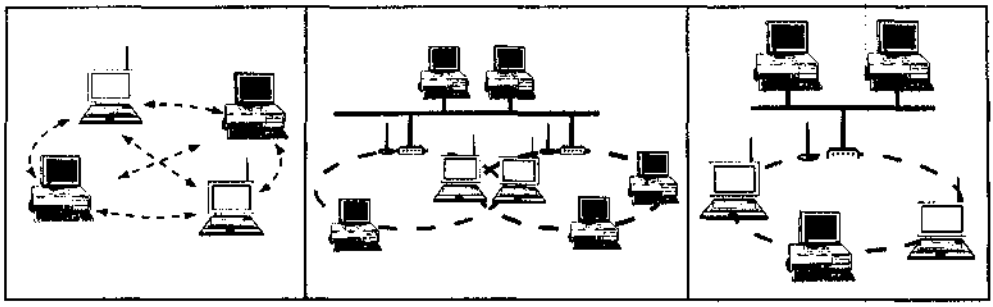


Рис. 2.6. Радиосеть для офисного применения

рованному пункту управления указание добавить молоко в список покупок). При этом одними из немаловажных параметров новой технологии являются: низкая стоимость устройства связи, небольшие размеры (ведь речь идет о мобильных устройствах) и, что немаловажно, совместимость, простота встраивания в различные устройства.

Технология Bluetooth использует небольшие приемопередатчики низкой мощности малого радиуса действия либо непосредственно встроенные в устройство, либо подключаемые через свободный порт или PC-карту. Они работают на не лицензируемой во всем мире частоте 2,45 ГГц, так называемого, ISM-диапазона (Industry, Science, Medicine — Диапазон промышленного, научного и медицинского применения), что позволяет свободно использовать устройства Bluetooth во всем мире.

Радиус действия устройств Bluetooth составляет около 10 м (в перспективе предполагается увеличить это расстояние до 100 м), при этом допускается наличие препятствий между соединяемыми устройствами (стены, мебель и т. п.). Если приемное устройство обнаруживает, что передатчик находится ближе чем в 10-и метрах, оно автоматически снижает мощность передачи. Устройство должно также переключаться в режим низкой мощности, как только объем трафика станет снижаться или вовсе прекратится.

Bluetooth-устройства способны связать вместе до 256-и устройств, из которых одновременно работают 8 (один — в режиме ведущего, 7 — в режиме ведомых), а остальные находятся в режиме ожидания. Радиоканал обеспечивает скорость передачи информации 721 кбит/с и передачу трех голосовых каналов. Технология использует FHSS — скачкообразную перестройку частоты (1600 скачков/с) с расширением спектра. При работе передатчик переходит с одной рабочей частоты на другую по псевдослучайному алгоритму. Используется дуплексный режим с временным разделением (TDD). Поддерживается изохронная и асинхронная передача данных и обеспечивается простая интеграция с TCP/IP. Временные интервалы (Time Slots) развертываются для синхронных пакетов, каждый из которых передается на своей частоте.

Абонентские устройства Bluetooth объединяются в группы (пикосети), коллективно использующие один и тот же радиоканал. В состав каждой пикосети входят один ведущий приемопередатчик (с опорным генератором, который синхронизирует внутренний трафик сети) и до семи ведомых (синхронизируемых). Все опорные генераторы в сети имеют фиксированную настройку. Ведомое устройство вычисляет разность между частотами собственного и ведущего генераторов; в процессе синхронизации эта погрешность учитывается, что обеспечивает точное соответствие излучаемой частоты данного и ведущего устройств.

Все устройства в пикосети равноправны и обладают одинаковыми возможностями (в отличие от сотовых сетей, где базовая станция принципиально отличается от абонентской как по пропускной способности, так и по составу технических средств). Разница состоит лишь в статусе устройств: ведущее или ведомые.

Все ведомые устройства находятся в дежурном режиме (режиме ожидания), регулярно включаясь по заданной программе. После «пробуждения» приемник осуществляет поиск контрольной несущей частоты (wake-up carrier), периодически излучаемой ведущим устройством. Если обнаруживается полезный сигнал, устройство автоматически переходит из режима ожидания в рабочее состояние.

Технология Bluetooth рассматривается многими разрабочиками как партнерская технология универсальной радиосвязи для локальных сетей. Сейчас уже появились передатчики, подключаемые через PC-карту и порт USB.

Контроль мобильных средств связи

Не секрет, что изначально беспроводные радиосети разрабатывались для офисных применений, но, как оказалось, на базе такого оборудования можно создавать хорошо работающие сети в масштабах города.

Как правило, на начальном этапе строительства таких сетей создаются несколько базовых станций с круговой диаграммой направленности, накрывающих всю территорию обслуживания. В дальнейшем, с увеличением числа пользователей, для снижения нагрузки на сеть разворачиваются дополнительные базовые станции. В идеальном случае сеть должна состоять из большого числа базовых станций с малым радиусом действия, но тогда возникает проблема взаимных помех от соседних базовых станций. Тем не менее современное радиооборудование позволяет решать эту проблему. Пример одного из вариантов широкомасштабной радиосети представлен на рис. 2.7.

Современные средства беспроводной персональной связи несоизмеримо расширяют нашу свободу, освободив нас от постоянного нахождения за рабочим столом, дают нам возможность в любое время и в любом месте связаться с необходимым корреспондентом, чтобы получить необходимую информацию. Но немногие знают, что эти чудеса техники скрывают в себе опасные ловушки. Для того чтобы однажды ваш помощник (ваше средство связи) не превратился в вашего врага, об этих ловушках необходимо знать все.

Современные беспроводные средства персональной связи — это и мобильные телефоны сотовой связи, и пейджеры, и радиостанции, и беспроводные стационарные радиотелефоны.

Проблема безопасности при пользовании сотовым телефоном и другими мобильными средствами персональной беспроводной связи имеет два аспекта:

- физическую безопасность пользователя;
- безопасность информации, передаваемой с помощью этих устройств.

Здесь мы рассмотрим только вопросы, касающиеся информационной безопасности. В настоящее время электронный перехват информации, циркулирующей в сотовых, беспроводных радиотелефонах или пейджерах, стал широко распространенным явлением.

Чтобы лучше понять проблемы, связанные с использованием беспроводных средств связи, вспомним, какие это средства и как они работают.

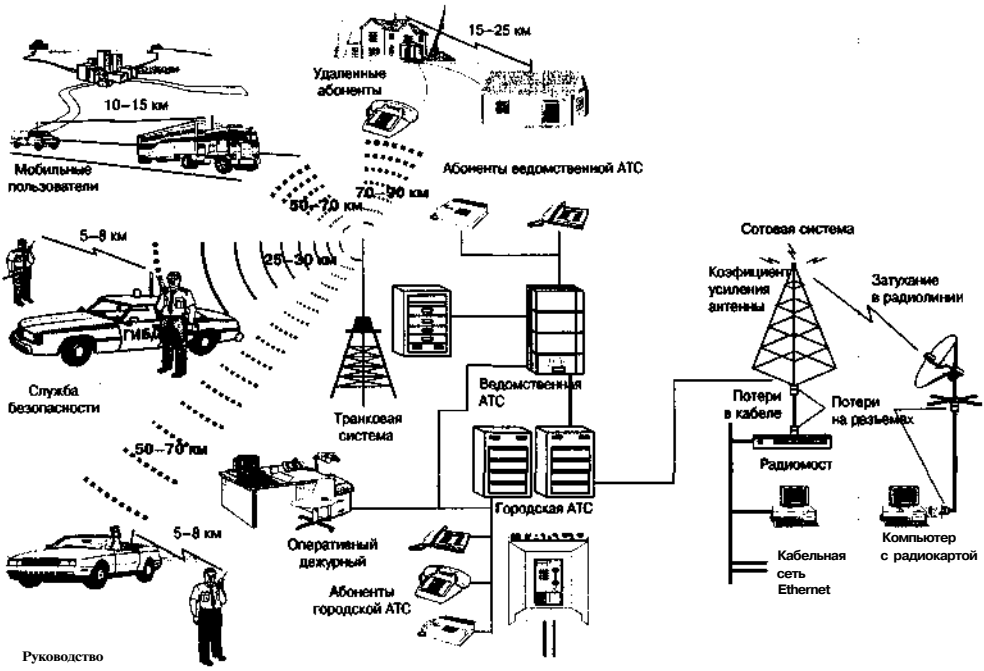


Рис. 2.7. Широкомасштабная радиосеть

Пейджеры представляют собой мобильные радиоприемники с устройством регистрации сообщений в буквенном, цифровом или смешанном представлении, работающие в основном в диапазоне 140-400 МГц. Система пейджинговой связи принимает сообщение от телефонного абонента, кодирует его в нужный формат и передает на пейджер вызываемого абонента.

Стационарный беспроводный радиотелефон объединяет в себе обычный проводной телефон, представленный самим аппаратом, подключенным к телефонной сети, и приемо-передающее устройство в виде телефонной трубки, обеспечивающей двусторонний обмен сигналами с базовым аппаратом. В зависимости от типа радиотелефона, используемого диапазона частот, мощности передатчика и чувствительности приемника (с учетом наличия помех и переотражающих поверхностей) дальность связи между трубкой и базовым аппаратом в помещении составляет в среднем до 50 м, а в зоне прямой видимости может достигать 3 км.

Мобильные телефоны сотовой связи фактически являются сложной миниатюрной приемо-передающей радиостанцией. При изготовлении каждому сотовому телефонному аппарату присваивают электронный серийный номер, кодируемый в микрочипе телефона, который затем изготовители аппаратуры сообщают специалистам, обслуживающим сотовый телефон. Кроме того, некоторые изготовители указывают этот номер в руководстве пользователя. При подключении аппарата к сотовой системе связи техники компании, предоставляющей услуги этой связи, дополнительно заносят в микрочип телефона еще и мобильный идентификационный номер.

Мобильный сотовый телефон обладает большой, а иногда и неограниченной, дальностью действия, которую обеспечивает сотовая структура зон связи. Вся территория, обслуживаемая сотовой системой связи, разделена на прилегающие друг к другу зоны связи, или соты. Телефонный обмен в каждой такой соте управляется базовой станцией, способной принимать и передавать сигналы на многих радиочастотах. Кроме того, эта станция подключена к обычной проводной телефонной сети и оснащена аппаратурой преобразования ВЧ-сигнала сотового телефона в НЧ-сигнал проводного телефона, и наоборот, за счет чего обеспечивается сопряжение обеих систем.

Периодически базовая станция излучает в эфир служебный сигнал. Приняв его, мобильный телефон автоматически добавляет к нему свои серийный и идентификационный номера и передает получившуюся кодовую комбинацию на базовую станцию. В результате этого осуществляются идентификация конкретного сотового телефона, номера счета его владельца и привязка аппарата к определенной зоне, в которой он находится в данный момент. Когда пользователь звонит по своему телефону, базовая станция выделяет ему одну из свободных частот той зоны, в которой он находится, вносит соответствующие изменения в его счет и передает его вызов по назначению. Если мобильный пользователь во время разговора перемещается из одной зоны связи в другую, базовая станция покидаемой зоны автоматически переводит сигнал на свободную частоту новой зоны.

С развитием технологий беспроводной передачи данных и мобильного доступа в Internet современные сотовые телефоны приобретают свойства персональных компьютеров. Скоро в каждом мобильном телефоне будет своя операционная система, текстовые редакторы, базы данных. Все это даст пользователям возможность создавать файлы и обмениваться ими. С помощью телефонных аппаратов становятся возможными ведение банковских операций, совершение интерактивных покупок, обмен электроннымиданными.

Созданию средств доставки информации из Internet на мобильные устройства способствовал протокол беспроводных приложений WAP (Wireless Application Protocol), который является одной из наиболее обсуждаемых технологий в мире мобильной связи. Тому есть несколько причин:

- ❑ данная технология является первым практическим шагом на пути объединения средств сотовой связи и глобальных компьютерных сетей;
- ❑ это первая попытка создать открытый стандарт для беспроводной передачи данных вне зависимости от поставщика как телефона, так и услуг, и способа связи;
- O WAP — протокол для беспроводного (через сотовый телефон) доступа, как правило, к специальным WAP-сайтам в Internet. Проще говоря, WAP-протокол — это стандартизированный способ связи мобильного телефона и сервера.

В отличие от иных способов доступа в Internet, когда сотовый телефон подключался через посредника, в роли которого выступал компьютер того или иного вида, данный протокол разрабатывался прежде всего для прямого доступа к сети с самого мобильного телефона посредством встроенного (в ПО телефона или SIM-карту) браузера.

По большому счету, работа сотового WAP-телефона в Internet принципиально ничем не отличается от работы простого браузера с простым сервером. Дополнительно лишь к стандартной связи по протоколу TCP/IP существует маршрутизатор WAP-Gateway, задачей которого является перевод запросов WAP-телефона в стандартную форму HTTP.

Для того чтобы воспользоваться WAP, необходимо заказать у оператора услугу передачи данных и соответствующим образом настроить телефон. При этом вы платите за время на линии, а соединение происходит на скорости не больше 9,6 кбит/с, что ограничивает возможности мобильного Internet. WAP проинформирует вас о расписании самолетов и поездов, пробках на дорогах, курсах валют, погоде, сообщит последние новости бизнеса, политики, культуры, спорта и даже программу телепередач центральных и спутниковых каналов. Такие сведения есть на серверах операторов сотовой связи и на серверах крупных Internet-порталов.

Надо сказать, что Internet-информация на экране мобильного телефона чем-то напоминает телетекст на миниатюрном телевизоре, однако благодаря возможности вводить информацию (заполнять простые текстовые формы) заметно расширяется сфера его применения.

Наиболее полезны и удобны услуги WAP, связанные с доступом к электронной почте. Благодаря им можно в любой момент просмотреть свежую корреспонденцию на дисплее сотового телефона. В последнее время такую услугу предоставляют крупнейшие бесплатные почтовые серверы. Проще говоря, WAP используется теми людьми, кому необходима краткая, но исчерпывающая текстовая информация, например, котировки ценных бумаг, банковские услуги и т. д.

Один из основных недостатков WAP — низкая скорость передачи информации 9,6 кбит/с. Он устраняется при передаче мультимедийной информации, используя стандарт GPRS (General Packet Radio Service), который позволяет увеличить эту скорость до 115,2 кбит/с и более.

Система GPRS обеспечивает мобильных пользователей высокой скоростью передачи данных и оптимально приспособлена для прерывистого трафика, характерного для сетей Internet/intranet. Она обеспечивает пакетную коммутацию на всем протяжении канала связи, существенно улучшая обслуживание в сетях стандарта GSM: соединения устанавливаются практически мгновенно, используются сетевые ресурсы, а участок частотного диапазона оказывается занятым только в моменты фактической передачи данных, что гарантирует чрезвычайно эффективное использование доступной полосы частот и позволяет делить один радиоканал между несколькими пользователями. Система поддерживает все самые распространенные протоколы передачи данных в сети, в частности Internet-протокол IP, за счет чего абоненты сети могут подключаться к любому источнику информации в мире.

К сожалению, бытует мнение, что сотовые радиотелефоны обеспечивают высокую безопасность передачи информации, поскольку каждый выход на связь абонентского аппарата происходит на другом канале (частоте) и, кроме того, каналы приема и передачи разнесены между собой. Это в еще большей степени касается сотовых систем, использующих цифровые стандарты обработки сигналов. Однако существуют системы, состоящие из специализированного интеллектуального контроллера-демодулятора и приемника-сканера, управляемых портативным компьютером. Оператору достаточно лишь ввести номер интересующего его абонента — и комплекс будет автоматически записывать все входящие и исходящие звонки (переговоры), а также определять телефонные номера и сопровождать мобильный объект при переходе из соты в соту. Так ли это на самом деле?

Сотовый телефон — это замечательно, удобно и практично. Однако важно знать, что еще на этапе разработки закладываются следующие возможности любой аппаратуры сотовой связи:

- представление информации о точном местоположении абонента;
- запись и прослушивание разговоров;
- фиксация номеров, даты, времени, категории и т. д. вызывающей и принимающей вызов стороны;
- дистанционное включение микрофона для прослушивания.

Немногие знают, что наличие мобильного сотового телефона позволяет определить не только текущее местоположение владельца, но и проследить за всеми его перемещениями.

Текущее положение может выявляться двумя способами. Первый из них — обычный метод триангуляции (пеленгования), определяющий направление на работающий передатчик из нескольких (обычно трех) точек и дающий засечку местоположения источника радиосигналов. Необходимая для этого аппаратура обладает высокой точностью и вполне доступна.

Второй метод — через компьютер предоставляющей связь компании, который постоянно регистрирует, где находится абонент в данный момент даже тогда, когда он не ведет никаких разговоров (но идентифицирующим служебным сигналам, автоматически передаваемым телефоном на базовую станцию, о которых мы говорили выше). Точность определения местонахождения абонента в этом случае зависит от следующих факторов:

- топографии местности;
- наличия помех и переотражений от зданий;
- положения базовых станций;
- количества работающих в настоящий момент телефонов в данной соте;
- размера соты.

Анализ данных о сеансах связи абонента с различными базовыми станциями (через какую и на какую базовую станцию передавался вызов, дата вызова и т. п.) позволяет восстановить все перемещения абонента. Такие данные автоматически регистрируются в компьютерах компаний, предоставляющих услуги сотовой связи, поскольку оплата этих услуг основана на длительности использования системы связи. В зависимости от фирмы, услугами которой пользуется абонент, эти данные могут храниться от 60 дней до 7 лет.

Такой метод восстановления картины перемещений абонента широко применяется полицией многих западных стран при расследованиях, поскольку дает возможность восстановить с точностью до минут, где был подозреваемый, с кем встречался (если у второго тоже был сотовый телефон), где и как долго происходила встреча, а также находился ли подозреваемый поблизости от места преступления в момент его совершения. Более того, в связи с тем, что алгоритмы кодирования и защиты в сотовых системах связи намеренно ослаблены (имеют дыры), информация, передаваемая по сотовой сети, становится легкой добычей для разного рода хакеров и проходимцев.

Электронный перехват сотовой связи не только легко осуществить, он к тому же не требует больших затрат на аппаратуру, и его почти невозможно обнаружить. На Западе прослушивание и/или запись разговоров, ведущихся с помощью беспроводных средств связи, практикуют правоохранительные органы, частные детективы, промышленные шпионы, представители прессы, телефонные компании, компьютерные хакеры и т. п. Например, в Канаде, по статистическим данным, от 20 до 80% радиообмена,

ведущегося с помощью сотовых телефонов, случайно или преднамеренно прослушивается посторонними лицами.

В западных странах уже давно известно, что мобильные сотовые телефоны, особенно аналоговые, являются самыми уязвимыми с точки зрения защиты передаваемой информации.

Принцип передачи информации такими устройствами основан на излучении в эфир радиосигнала, поэтому любой человек, настроив соответствующее радиоприемное устройство на ту же частоту, может услышать каждое ваше слово. Для этого даже не нужна сложная аппаратура. Разговор, ведущийся с сотового телефона, можно прослушать с помощью программируемых приемников-сканеров с полосой приема 30 кГц, способных осуществлять поиск в диапазоне 450-1900 МГц.

Перехватывать информацию с аналоговых неподвижных и стационарных сотовых телефонов легко, с мобильных — труднее, так как перемещение абонента в процессе разговора сопровождается снижением мощности сигнала и переходом на другие частоты в случае передачи сигнала с одной базовой станции на другую.

Более совершенны с точки зрения защиты информации цифровые сотовые телефоны, передающие информацию в виде цифрового кода. Однако используемый в них алгоритм шифрования может быть вскрыт опытным специалистом в течение нескольких минут с помощью персонального компьютера. Что касается цифровых кодов, набираемых на клавиатуре цифрового сотового телефона (телефонные номера, номера кредитных карточек или персональные идентификационные номера), то их легко перехватить с помощью того же цифрового сканера.

Не менее уязвимы беспроводные радиотелефоны. При работе они используют две радиочастоты: одну — для передачи сигнала от аппарата к трубке, другую — от трубки к аппарату. Наличие двух частот еще больше расширяет возможности для перехвата. Дальность перехвата, в зависимости от конкретных условий, составляет в среднем до 400 м, а при использовании дополнительной дипольной антенны диапазона — до 1,5 км.

Следует отметить, что часто рекламируемые возможности беспроводного телефона — цифровой код безопасности (digital security code) и снижение уровня помех (interference reduction) — нисколько не предотвращают возможность перехвата разговоров. Они только препятствуют несанкционированному использованию этого телефона и не позволяют соседним радиотелефонам звонить одновременно. Сложнее перехватить информацию с цифровых радиотелефонов, которые могут использовать при работе от 10 до 30 частот с автоматической их сменой по определенному закону. Однако для специалиста и такой перехват не представляет особой трудности.

Уязвимыми в отношении безопасности передаваемой информации являются и пейджеры. В большинстве своем они используют протокол POCSAG, который практически не обеспечивает защиты от перехвата. Сообщения в пейджинговой системе связи можно перехватить с помощью радиоприемников или сканеров. Существует также целый ряд программных средств, которые позволяют компьютеру в сочетании со сканером автоматически захватывать рабочую частоту нужного пейджера или контролировать весь обмен в конкретном канале пейджинговой связи. Эти программы предусматривают возможность перехвата информации с 5000 пейджеров одновременно и обеспечить ее хранение в своей памяти.

Различают узкополосные (аналоговые) и широкополосные (цифровые) каналы передачи сообщений.

Узкополосный канал — это стандартный канал, не обладающий частотной избыточностью. Любое преобразование речевых сигналов и данных не должно приводить к существенному расширению спектра передаваемого сигнала.

Для широкополосных каналов полоса спектра сигнала существенно больше полосы спектра сообщения, поэтому возможности таких каналов значительно шире, чем узкополосных.

Любые преобразования в канале связи сопровождаются погрешностями, обусловленными влиянием различного рода дестабилизирующих факторов и помех. В связи с этим наряду с решением проблемы защиты информации важно обеспечение качества восстановленного сообщения.

Радиочастотное общение (переговоры) производится, как правило, с помощью специальных радиостанций и радиотелефонов, в том числе и сотовых, действующих преимущественно в диапазоне УКВ.

Радиотелефон — это радиостанция, функционирующая в паре с телефонной линией, причем вся эта система может быть либо сугубо индивидуальной (радиоудлинители), либо групповой (сотовой и транковой).

Практика радиообщения зависит от конструкции аппаратуры и осуществляется как на единой общей частоте, так и на разных; как одновременно, т. е. дуплексно, без переключения «прием-передача», так и поочередно, т. е. симплексно с таковым переключением.

Для перехвата радиопереговоров надо знать несущую частоту радиопередачи, на которую в ходе прослушивания и настраивают свою аппаратуру. Если же рабочая частота передатчика неизвестна (некоторую ориентацию здесь способны дать габариты и конструкция применяемых антенн), то пытаются выявить момент радиосвязи и внимательно просканировать весь диапазон широковолновым радиоприемником (сканером), засекая нужную волну по нюансам разговора или голосу говорящего по телефону. Иногда подобный перехват удается провести посредством телевизионного или вещательного ЧМ-приемника либо зарубежного «сэконд-хэндового» радиотелефона.

Зная, что прием и передача зачастую происходят на различных частотах, целесообразно иметь под рукой два радиоприемника, каждый из которых наблюдает за отдельной полосой контролируемого диапазона.

Так как факт радиоперехвата нельзя засечь, для нейтрализации подобной неприятности разработаны уловки вроде кодирования радиосигналов или резко «прыгающей» частоты. Встретившись с такими изощрениями, проще будет не преодолевать их, а переходить на иные пути добычи требующейся информации.

Никто не спорит, сотовые телефоны, пейджеры и просто радиостанции очень полезны, особенно если абонент постоянно в пути. Поэтому все современные виды связи так быстро внедряются в повседневную жизнь любого делового человека, а не только «нового русского». Однако все шире осваивая образцы западной техники, мы крайне редко задумываемся о том, какую угрозу несет подобное техническое новаторство.

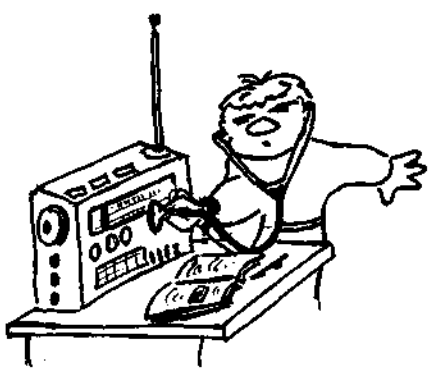
Способы НСД с использованием побочных электромагнитных излучений и наводок

Проблема утечки информации из средств вычислительной техники через побочные электромагнитные излучения и наводки (ПЭМИН) известна специалистам уже на протяжении нескольких десятков лет. И только в последние годы она стала обсуждаться на страницах открытой литературы. Это связано, прежде всего, с широчайшим распространением персональных компьютеров и других средств обработки информации. Практически любая организация, будь то коммерческая фирма или государственное предприятие, сегодня не может существовать без использования такой техники.

Термин перехват побочных электромагнитных излучений означает получение необходимой информации за счет приема электромагнитных сигналов пассивными средствами, расположенными, как правило, на достаточно безопасном расстоянии от источника конфиденциальной информации.

Необходимо отметить, что практически все технические средства не только сами излучают в пространство сигналы, содержащие обрабатываемую ими информацию, но и улавливают за счет микрофонов либо антенн другие излучения (акустические, электромагнитные), существующие в непосредственной близости от них. Уловив, они преобразовывают принятые излучения в электрические сигналы и бесконтрольно передают их по своим линиям связи на значительные расстояния. Это еще больше повышает опасность утечки информации. К числу технических устройств, способных образовывать электрические каналы утечки, относятся телефоны (особенно кнопочные), компьютеры, средства громкоговорящей связи, радиотрансляционные приемники, датчики охранной и пожарной сигнализации, а также их линии и сети электропроводки.

С помощью чувствительной радиоэлектронной аппаратуры возможен прием побочных электромагнитных излучений и наводок, а затем полное восстановление информации, которая обрабатывается компьютерами, принтерами, мониторами и другой офисной техникой. Частотный диапазон информационных излучений простирается от десятков килогерц до гигагерцев и определяется тактовой частотой техники, используемой для обработки информации. Например, перехват информации мониторов возможен на частотах вплоть до 10-15 гармоники тактовой частоты, но максимум информационных излучений обычно приходится на диапазон 100—350 МГц.



Следует иметь в виду, что перехват информации возможен на каждой гармонике тактовой частоты, излучаемой в пространство с достаточной интенсивностью. Пример спектрограмм побочных информационных излучений различной офисной техники представлен на рис. 2.8.

Говорить о какой-либо диаграмме направленности электромагнитных излучений в данном случае не приходится, так как на практике состав-

ные части, например, компьютера (системный блок, монитор, соединительные кабели и провода питания) могут как угодно располагаться относительно друг друга. Поляризация излучений компьютера — линейная. В конечном счете она определяется расположением соединительных кабелей, так как именно они являются основными источниками излучений в компьютерах, у которых системный блок имеет металлический кожух.

Распространение побочных электромагнитных излучений за пределы контролируемой территории создает предпосылки для утечки информации, так как возможен ее перехват с помощью специальных технических средств. В компьютере основными источниками электромагнитных излучений являются монитор и соединительные цепи (устройства ввода и вывода информации). Утечке информации в компьютере и другой технике способствует применение коротких видеоимпульсов прямоугольной формы и высокочастотных коммутирующих сигналов.

Если, работая на компьютере, вы одновременно включали телевизор, то, наверное, заметили, что при включенном компьютере на некоторых телевизионных каналах начинаются помехи. Этому есть простое объяснение. Все составляющие части компьютера (провода, усилители, даже печатные платы) работают как антенны, проводящие электромагнитное излучение. Компьютер не только принимает излучение, но и передает, иногда перенося его на некоторое расстояние от источника, а близлежащая электропроводка и металлические трубки могут впоследствии работать как антенны.

Что касается уровней побочных электромагнитных излучений вычислительной техники, то они регламентированы с точки зрения электромагнитной совместимости зарубежными и отечественными стандартами. Например, согласно публикации № 22 CISPR (Специальный Международный Комитет по Радиопомехам) для диапазона 230—1000 МГц уровень напряженности электромагнитного поля, излучаемого оборудованием вычислительной техники, на расстоянии 10 м не должен превышать 37 дБ. Очевидно, что этот уровень излучения достаточен для перехвата на значительных расстояниях.

Таким образом, соответствие электромагнитных излучений средств вычислительной техники нормам на электромагнитную совместимость не является гарантией сохранения конфиденциальности обрабатываемой в них информации. Кроме того, надо заметить, что значительная часть парка компьютеров в России не отвечает даже этим

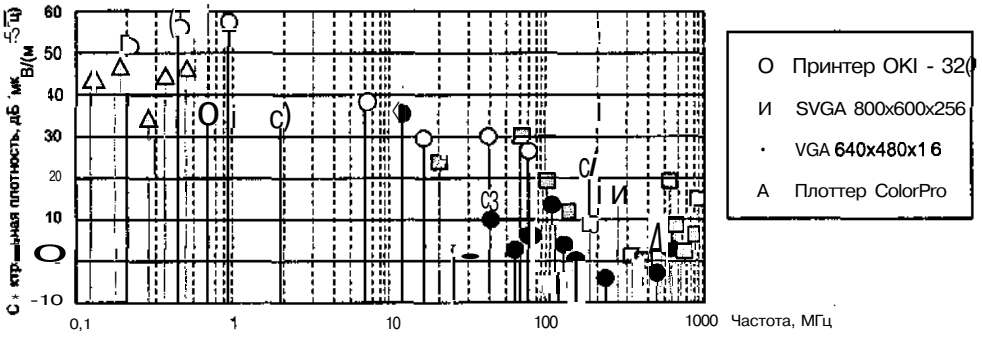


Рис. 2.8. Спектрограммы побочных информационных излучений

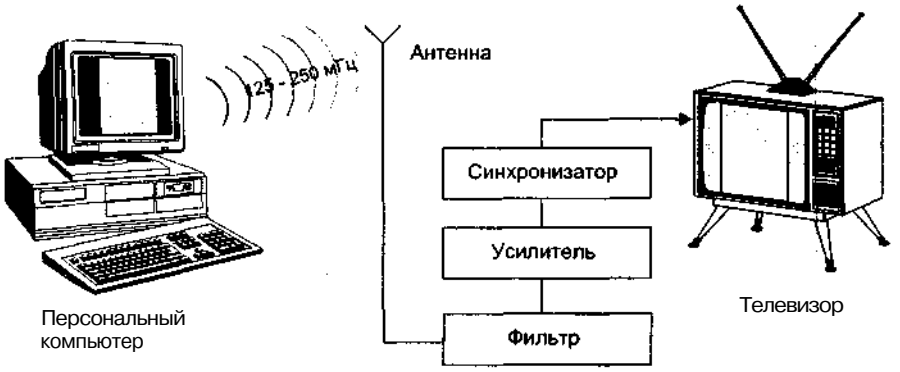


Рис. 2.9. Устройство для снятия информации с компьютера

нормам, так как в погоне за дешевизной в страну ввозили технику в основном «желтой» сборки, не имеющую сертификатов качества.

Самым мощным источником излучения в компьютере является система синхронизации. Однако перехват немодулированных гармоник тактовой частоты вряд ли сможет кого-нибудь заинтересовать. При использовании для перехвата ПЭМИН обычного бытового радиоприемника можно распознавать на слух моменты смены режимов работы компьютера, обращений к накопителям информации на жестком и гибком магнитных дисках, нажатий клавиш и т. д. Но подобная информация может быть использована только как вспомогательная и не более. Таким образом, не все составляющие побочного излучения персональных компьютеров опасны с точки зрения реального перехвата обрабатываемой в них информации. Анализ лишь уровня электромагнитных излучений недостаточен для восстановления информации. Нужно еще знать их структуру. Поэтому в техническом плане проще решается задача перехвата информации, отображаемой на экране монитора.

Исследования показывают, что излучение видеосигнала монитора является достаточно мощным, широкополосным и охватывает диапазон метровых и дециметровых волн. Причиной мощного излучения является наложение радиосигнала на импульсы развертки изображения, вырабатываемые строчным трансформатором. При кажущейся сложности проблемы аппаратура для этого вида коммерческой разведки достаточно проста (рис. 2.9). Ее изготавливают на базе обычного малогабаритного телевизора.

Такие устройства позволяют на удалении 50 м получать устойчивую картинку, отображаемую в настоящий момент на экране монитора вашего компьютера. Она может быть восстановлена в монохромном виде. При этом изображения текста можно восстановить с лучшим качеством. Выделение из ПЭМИН-компьтера информации о сигнале синхронизации изображения представляет собой довольно сложную техническую задачу. Гораздо проще эта проблема решается с использованием внешних перестраиваемых генераторов синхросигналов.

Все компьютеры работают на излучение в широком радиочастотном диапазоне и представляют собой радиопередатчики. Когда телевидение принимает сигналы от компьютера, это происходит случайно; а теперь представьте себе, что кто-то решил целенаправленно принимать такую излучаемую информацию. Конечно же это возможно, и

такие случаи бывали. Недаром компьютеры с засекреченной информацией устанавливают в комнатах с непроницаемыми для излучения стенами.

Исследования в этой области показывают, что на экране телевизионного устройства можно последовательно читать тексты с любого из 10—15 одновременно работающих мониторов или постоянно считывать информацию с одного из них

Рассмотрим это явление более подробно. Работа любой вычислительной техники сопровождается электромагнитными излучениями и наводками на соединительные проводные линии, цепи «питание» и «земля», возникающие вследствие электромагнитных воздействий в ближней зоне излучения. Считалось, что достаточно трудно расшифровать информацию, содержащуюся в излучении, и что поэтому восстановление информации под силу только профессионалам, располагающим очень сложной и дорогой аппаратурой обнаружения и декодирования. Однако это оказалось не так.

Применение в компьютерах импульсных сигналов прямоугольной формы и ВЧ-коммутации приводит к тому, что в спектре излучений будут присутствовать компоненты с частотами вплоть до СВЧ. Импульсы — вот ключевое слово. Всем известно, что компьютеры способны преобразовывать длинные строки нулей и единиц во что угодно (например, в наши любимые компьютерные игры). На самом деле, разумеется, по проводам не «бегают» крошечные нули и единички. По ним просто течет электрический ток различного напряжения, который наше воображение представляет как нули и единички.

Любой электрический прибор является источником излучения. Но только цифровой прибор (например компьютер) испускает импульсы высокого и низкого уровня напряжения. Энергетический спектр таких сигналов убывает с ростом частоты, но эффективность излучения при этом увеличивается и уровень излучений может оставаться постоянным до частот в несколько гигагерц (рис. 2.10). Усиление излучения на некоторых частотах спектра (резонанс) может вызвать различные паразитные связи. Цепи, не предназначенные для передачи цифровых сигналов, могут излучать их вследствие наводок, например, провода источников питания.

Изображение на экране монитора формируется в основном так же, как и в телевизиоре. Оно состоит из множества крошечных точек, называемых пикселами. Каждый пиксел представляет собой капельку определенного вещества, которая светится (флу-

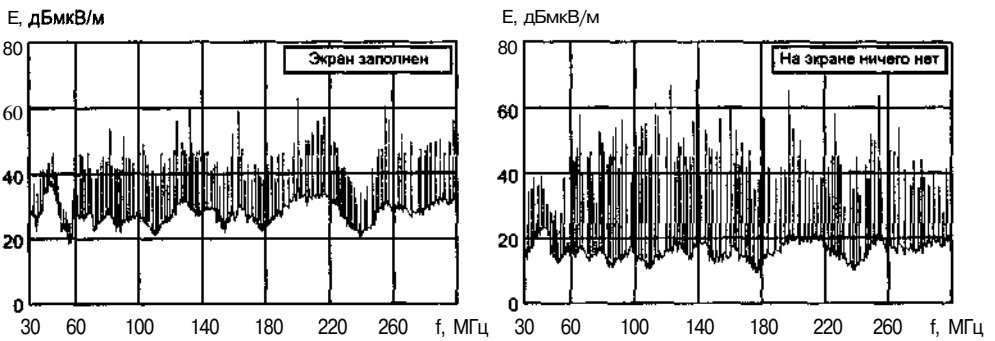


Рис. 2.10. Напряженность электрического поля E на расстоянии 1 м м от дисплея

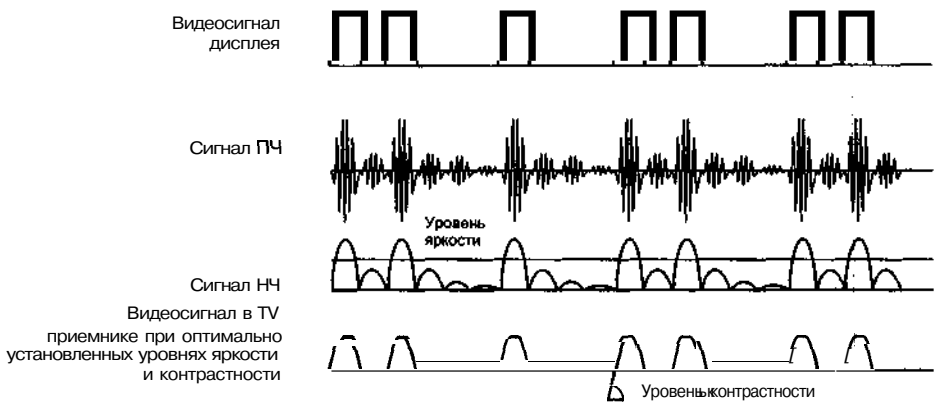


Рис. 2.11. Временные диаграммы сигналов, обрабатываемых ТВ-приемником

оресцирует) под воздействием энергии и покрыта защитным слоем. Контролирующая схема управляет позицией электронной пушки, которая периодически простреливает электронами весь экран, на короткое время зажигая те пикселы, которые должны засветиться. Каждый раз, когда это происходит, мы регистрируем импульс электромагнитного излучения с высоким напряжением. Поскольку видеосигнал является цифровым, то логическая единица соответствует светящейся точке, а логический нуль препятствует ее появлению. Однако видеосигнал содержит еще и тактовые синхроимпульсы. Так как последние повторяются, то энергетический спектр видеосигнала содержит гармоники, интенсивность которых убывает с ростом частоты. Источниками излучения видеосигнала дисплея могут быть элементы обработки сигнала изображения и электронный луч кинескопа. Уровень этих сигналов усиливается до нескольких десятков вольт для подачи на электронно-лучевую трубку.

Уровень широкополосного излучения дисплея зависит от количества букв на экране. Уровень узкополосных составляющих не зависит от заполнения экрана, а определяется системой синхронизации и частотой повторения светящихся точек. Поэтому бывает очень трудно, а подчас и невозможно, отделить различные сигналы друг от друга и расшифровать их. Вам вряд ли удастся узнать, о чем же «думал» компьютер, пока систему сотрясали электромагнитные импульсы. Как же расшифровать всю эту принимаемую мешанину сигналов, исходящих от проводов, печатных плат и т. д.?

Информация, отображаемая на экране дисплея, может быть восстановлена с помощью телевизионного приемника, который обрабатывает лишь небольшую часть спектра сигнала шириной около 8 МГц (обычно ТВ-приемник имеет полосу пропускания 4,5 МГц и демодулятор сигнала с частично подавленной боковой полосой, эквивалентной АМ-детектору с полосой пропускания 8 МГц) на частотах в диапазонах метровых и дециметровых волн. Временные диаграммы сигналов, обрабатываемых ТВ-Приемником, представлены на рис. 2.11.

Рис. **2.12.** Видеосигналы в дисплее и ТВ-приемнике

Пусть ТВ-приемник обрабатывает один «лепесток» энергетического спектра излучения, то есть частота его настройки совпадает с серединой одного из «лепестков», а полоса пропускания равна его ширине. Усиление НЧ-сигнала над порогом, определяющим яркость, задается уровнем контрастности. В первом приближении уровень контрастности определяет крутизну фронтов видеосигнала в приемнике. В отличие от дисплея, максимум видеосигнала в ТВ-приемнике определяет уровень черного, а минимум — уровень белого. Таким образом, изображение на экране ТВ-приемника будет представлять собой копию изображения на экране дисплея, состоящую из черных символов на белом (или сером) фоне.

Если видеосигнал представляет собой длинный импульс, то лучше будут излучены в пространство его фронты, которые и дадут при приеме точки (рис. 2.12).

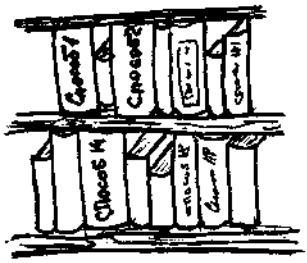
Излучение дисплея, принимаемое ТВ-приемником, не содержит информации о синхросигнале, поэтому изображение на экране телевизора будет перемещаться в горизонтальном и вертикальном направлениях. Качество приема можно улучшить, если использовать внешний генератор синхросигналов. С такой приставкой к обычному телевизору можно восстановить информацию с дисплея почти любого типа при условии достаточно высокого уровня его излучения.

Кроме электромагнитных излучений, вблизи устройств вычислительной техники всегда присутствуют квазистатические информационные магнитные и электрические поля, быстро убывающие при увеличении расстояния, но вызывающие наводки на близко расположенные отходящие цепи (охранная сигнализация, телефонные провода, сеть питания, металлические трубы и т. д.). Такие поля существенны в диапазоне частот от десятков килогерц до десятков мегагерц. Перехват информации в этом случае возможен при непосредственном подключении специальной приемной аппаратуры к этим коммуникациям за пределами охраняемой и контролируемой территории.

Надо знать также, что телефоны с кнопочным набором номера сами являются источниками паразитных радиоизлучений, поэтому разговоры, проводимые с применением некоторых из них, можно пробовать засечь на частоте ДВ-диапазона (около 150 кГц) и дистанции в сотню-другую метров.

Способы НСД к компьютерам, сетевым ресурсам и программному обеспечению

В настоящее время проблемы информационной безопасности постоянно усугубляются вследствие проникновения технических средств обработки и передачи данных и, прежде всего, информационно-вычислительных систем практически во все сферы деятельности общества. Хакеры, «электронные корсары», «компьютерные пираты», набирая на удачу один номер за другим, терпеливо дожидаются, пока компьютер на другом конце провода не отзовется. После этого они подключают телефон к приемнику сигналов собственного персонального компьютера — связь установлена. Если теперь угадать код (а слова, которые служат паролем, часто банальны), то можно внедриться в чужую компьютерную систему.



Несанкционированный доступ к файлам законного пользователя осуществляется также путем обнаружения слабых мест в защите системы. Однажды выявив их, нарушитель может, не торопясь, исследовать содержащуюся в системе информацию, копировать ее, возвращаться к ней много раз.

В наши дни хакер может написать простенькую программу, которая выдает себя за клиента сетевой файловой системы NFS (Network File System), и, обходя обычные средства контроля доступа, получить прямой доступ к файлам пользователя. Система NFS — не единственное сетевое средство, уязвимое для подобного рода вмешательств; практически все сетевые модули имеют этот недостаток.

Программисты иногда допускают ошибки в программах, которые не удается обнаружить в процессе отладки. Авторы больших сложных программ могут не заметить некоторых слабостей логики их работы. Обычно слабости все-таки выявляются при проверке, редактировании, отладке программы, но абсолютно избавиться от них невозможно. Кроме того, уязвимые места иногда обнаруживаются и в электронных цепях, особенно в системах связи и передачи данных. Все эти небрежности и ошибки приводят к появлению существенных «брешей» в системах защиты информации.

Бывает, что некто проникает в компьютерную систему, выдавая себя за законного пользователя. Системы, которые не обладают средствами аутентичной идентификации (например, по физиологическим характеристикам: по отпечаткам пальцев, по рисунку сетчатки глаза, голосу и т. п.), оказываются без защиты против этого приема. Самый простейший путь его осуществления — получение кодов и других Идентифицирующих шифров законных пользователей. Это может производиться следующими способами:

- приобретением (обычно подкупом персонала) списка пользователей со всей необходимой информацией;
- обнаружением такого документа в организациях, где не налажен достаточный контроль за их хранением;
- подслушиванием через телефонные линии.

Иногда случается (как, например, с ошибочными телефонными звонками), что пользователь с удаленного терминала подключается к чьей-то системе, будучи абсолютно уверенным, что он работает с той системой, с какой и намеревался. Владелец системы, к которой произошло фактическое подключение, формируя правдоподобные отклики, может поддерживать это заблуждение в течение некоторого времени и таким образом получить информацию, в частности, коды.

Способы НСД к компьютерам и сетевым ресурсам

Проблема защиты информации от несанкционированного доступа стала значительно острее, когда получили широкое распространение локальные и, особенно, глобальные компьютерные сети. Основной целью хакеров, по мнению специалистов, является сбор большого количества имен пользователей и паролей входа. Как правило, их не интересуют коммерческие тайны, хотя некоторым хакерам удавалось прорваться в сети

крупных компаний, разрабатывающих программные продукты, внедряться в телекоммуникационные сети банков, учреждения министерства обороны и т. п.

Одним из беспрецедентных компьютерных преступлений в последние годы стал взлом многослойной защиты компьютерной системы банка «Сити-банк» (США, Нью-Йорк). Российский гражданин В. Левин с 30 июня по 3 октября 1994 года, находясь в Санкт-Петербурге и используя обычный персональный компьютер и электронную связь, произвел не менее 40 незаконных переводов на общую сумму около 12 млн долларов со счетов различных клиентов «Сити-банка» на счета действующих с ним в заговоре лиц или контролируемых ими фирм.

В США, например, ежегодные потери от компьютерной преступности оцениваются более чем на 100 млрд долларов, в странах Западной Европы — на 30 млрд. долларов. Средний и максимальный ущерб от одного компьютерного преступления составляет, соответственно, 450 тыс. и 1 млрд долларов. Ежегодные потери некоторых фирм США достигают 5 млрд долларов. Согласно статистическим данным, более 80% компаний и агентств несут финансовые убытки из-за недостаточно надежного обеспечения безопасности данных.

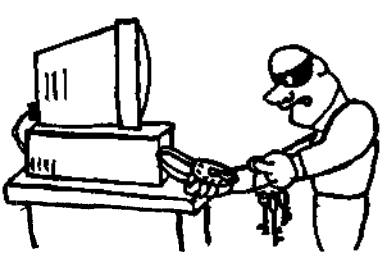
Одной из разновидностей несанкционированного доступа является подделка компьютерной информации, которая характеризуется тем, что пользоваться ею может, как правило, не посторонний пользователь, а сам разработчик, причем имеющий высокую квалификацию.

Идея преступления состоит в подделке выходной информации компьютеров с целью имитации работоспособности больших систем, составной частью которых является компьютер. Если подделка выполнена ловко, зачастую удается сдать заказчику заведомо неисправную продукцию.

К подделке информации можно отнести также подтасовку результатов выборов, голосования, референдумов и т. п. Каждый голосующий не может убедиться, что его голос зарегистрирован правильно, поэтому всегда можно внести искажения в итоговые протоколы. Естественно, что подделать информацию можно и другими целями.

К уязвимым местам в вычислительных сетях относятся:

- применение компьютеров, не имеющих парольной защиты во время загрузки;
- использование совместных или легко вскрываемых паролей;
- хранение паролей в пакетных файлах и на дисках компьютеров;
- отсутствие установления подлинности пользователя в реальном масштабе времени;
- отсутствие или низкая эффективность систем идентификации и аутентификации пользователей;
- недостаточность физического контроля за сетевыми устройствами;
- отсутствие отключения терминала при многочисленных неудачных попытках установления сеанса связи, а также регистрации таких попыток;
- незащищенность модемов.



Для защиты компьютерных сетей или отдельных компьютеров от несанкционированного использования применяются три основных вида контроля доступа, основанных на:

- владении физическим ключом;
- личностных характеристиках пользователя;
- обладании специфической информацией.

Когда говорят о контроле доступа, основанном на владении физическим ключом, речь идет о предметах, принадлежащих пользователю: физическом ключе, магнитной карте, металлической пластинке причудливой формы, которую вставляют перед началом работы в щель распознавателя.

Для контроля доступа, основанного на личностных характеристиках пользователя, используются биометрические приборы, анализирующие специфические физические особенности пользователя (подпись, тембр голоса, отпечатки пальцев, рисунок линий на ладони или на сетчатке глаза и т. п.) и сравнивают их с теми, что находятся в памяти приборов.

Компьютерная защита этих двух видов может использоваться и для дистанционного управления доступом, хотя обычно к ней прибегают для ограничения доступа к компьютерному залу или отдельному кабинету — помещению, где находятся компьютеры.

Контроль доступа, основанный на обладании специфической информацией, наиболее распространен и характеризуется тем, что правом доступа обладают лишь те лица, которые способны продемонстрировать свое знание определенного секрета, обычно — пароля. Это самый простой и дешевый способ защиты любой компьютерной системы. Поскольку его использование не требует больших затрат времени, сил, а также памяти компьютера, то он применяется даже в тех компьютерах, которые вовсе не нуждаются в средствах защиты.

Кроме того, использование пароля дает пользователю ощущение психологического комфорта. Этот способ защиты широко используется в системах, уже защищенных другими средствами — магнитными картами или иными программными методами типа шифрования, — это в еще большей степени укрепляет защиту от несанкционированного доступа.

Пароли, как правило, рассматриваются в качестве ключей для входа в систему, но они используются и для других целей: блокирование записи на дисковод, в командах на шифрование данных, то есть во всех тех случаях, когда требуется твердая уверенность, что соответствующие действия будут производиться только законными владельцами или пользователями программного обеспечения.

Пароли можно подразделить на семь основных групп (рис. 2.13):

- пароли, устанавливаемые пользователем;
- пароли, генерируемые системой;
- случайные коды доступа, генерируемые системой;
- полуслова;
- ключевые фразы;
- интерактивные последовательности типа «вопрос — ответ»;
- «строгие» пароли.

Пароли первой группы применяются наиболее часто. Большинство таких паролей относятся к типу «выбери сам». Для более надежной защиты от несанкционированного доступа необходимо использовать достаточно длинный пароль, поэтому обычно система запрашивает пароль, содержащий не менее четырех-пяти букв. Существуют и

другие меры, не позволяющие пользователю создать неудачный пароль. Например, система может настаивать на том, чтобы пароль включал в себя строчные и заглавные буквы вперемешку с цифрами; заведомо очевидные пароли, например, Internet, ею отвергаются.

В разных операционных системах существует немало программ, которые просматривают файлы, содержащие пароли, анализируют пароли пользователей и определяют уровень их секретности. Неподходящие пароли заменяются или удаляются.

Представьте себе состояние человека, когда он впервые загружает компьютер, и компьютер просит его ввести собственный секретный пароль. Стоит запросу появиться на экране монитора, и человека посещает мысль о том, что надо немедленно что-то предпринимать. Не считая гениев и безнадежных тупиц, все люди, когда надо принимать быстрые решения, мыслят и действуют примерно одинаково. Им требуется время, чтобы начать мыслить творчески, поэтому начальные предположения и первые умозаключения в определенных группах людей оказываются одинаковыми. И пользователи выдают первое, что приходит им в голову. А в голову приходит то, что они видят или слышат в данный момент, либо то, что собираются сделать сразу же после загрузки. В такой ситуации пароль создается в спешке, а последующая его замена на более надежный происходит довольно редко. Таким образом, многие пароли, созданные пользователями, могут быть раскрыты достаточно быстро.

Пароли и коды, устанавливаемые системой, могут быть нескольких разновидностей. Системное программное обеспечение может использовать полностью случайную последовательность символов (вплоть до случайного выбора регистров, цифр, пунктуации длины) или же применять какие-либо ограничения в генерирующих процедурах. Компьютер может создавать пароли, случайным образом извлекая из списка обычных или ничего не значащих слов, созданных авторами программы, и образовать нечто вроде onah.foopn или ocar-back-treen.

Полуслова частично создаются пользователем, а частично — каким-либо случайным процессом. Это значит, что если даже пользователь придумает легкоугадывае-

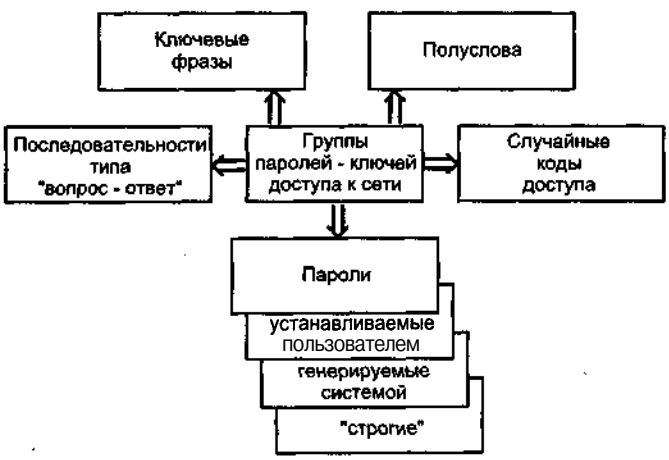


Рис. 2.13. Основные группы формирования паролей для доступа к сети

мый пароль, например, «абзац», компьютер дополнит его какой-нибудь неразберихой, образовав более сложный пароль типа «абзац,3ю37».

Ключевые фразы хороши тем, что они длинные и их трудно угадать, зато легко запомнить. Фразы могут быть осмысленными, типа «мы были обеспокоены этим», или не иметь смысла — «ловящий рыбу нос». Следует заметить, что в программировании постепенно намечается тенденция к переходу на более широкое применение ключевых фраз.

К концепции ключевых фраз близка концепция кодового акронима, который эксперты по защите оценивают как короткую, но идеально безопасную форму пароля. В акрониме пользователь берет легко запоминающееся предложение, фразу, строчку из стихотворения и т. п., и использует первые буквы каждого слова в качестве пароля. Например, акронимами двух приведенных выше фраз являются «мбоэ» и «лрн». Подобные нововведения в теории паролей значительно затрудняют электронный шпионаж.

Интерактивные последовательности «вопрос — ответ», предлагают пользователю ответить на несколько вопросов, как правило, личного плана: «Девичья фамилия вашей матери?», «Ваш любимый цвет?» и т. д. В компьютере хранятся ответы на множество таких вопросов. При входе пользователя в систему компьютер сравнивает полученные ответы с «правильными». Системы с использованием «вопросов — ответов» склонны прерывать работу пользователя каждые десять минут, предлагая отвечать на вопросы, чтобы подтвердить его право пользоваться системой, В настоящее время такие пароли почти не используются. Когда их придумали, идея казалась неплохой, но раздражающие прерьшания привели к тому, что данный метод практически исчез из обихода.

«Строгие» пароли обычно используются совместно с каким-нибудь внешним электронным или механическим устройством. В этом случае компьютер обычно с простодушным коварством предлагает несколько вариантов приглашений, а пользователь должен дать на них подходящие ответы.

Пароли этого типа часто встречаются в системах с одноразовыми кодами. Одноразовые коды — это пароли, которые срабатывают только один раз. Их иногда используют, создавая временную копию для гостей, чтобы продемонстрировать потенциальным клиентам возможности системы. Они также порой применяются при первом вхождении пользователя в систему. Во время первого сеанса пользователь вводит новый собственный пароль, а в дальнейшем входит в систему лишь через него. Одноразовые коды могут также применяться в системе, когда действительный пользователь входит в нее в первый раз; затем пользователю следует поменять свой пароль на более засекреченный персональный код. Если системой пользуется группа людей, но при этом нельзя нарушать секретность, обращаются к списку одноразовых кодов, из которого тот или иной пользователь вводит код, соответствующий, например, времени, дате или дню недели.

Итак, для того чтобы пароль оказался действительно надежным, он должен отвечать определенным требованиям:

- ❑ быть определенной длины;
- ❑ включать в себя как прописные, так и строчные буквы;
- ❑ включать в себя одну и более цифр;
- ❑ включать в себя один нецифровой и один неалфавитный символ.

Нужно обязательно соблюдать одно или несколько из этих правил.

Чем же отличается несанкционированный доступ к компьютерным сетям от такого же несанкционированного доступа к их сетевым ресурсам (рис. 2.14). В первом случае некий субъект получает доступ на правах «законного» пользователя, используя различные уязвимые места сети.

Во втором случае несанкционированный доступ может произойти, в основном, по двум причинам: либо право доступа к ресурсам сети не определено должным образом, либо механизмы управления доступом и полномочиями недостаточно детализированы. Как правило, на практике довольно часто пользователям предоставляют более широкие права доступа к ресурсам сети, чем это необходимо, несмотря на ущерб безопасности информации.

К уязвимым местам доступа к ресурсам вычислительных сетей можно отнести:

- при назначении прав пользователей применение системных установок с недопустимо широким спектром полномочий;
- неправомерное использование полномочий администратора сети;
- неправильное использование механизма назначения полномочий для пользователей;
- использование компьютеров без механизма контроля доступа на уровне файлов;
- хранение данных без защиты или с недостаточным ее уровнем.

На примерах действий хакеров рассмотрим более детально, как же осуществляется несанкционированный доступ к компьютерам и сетям.

Лица, производящие несанкционированный доступ, а точнее, совершающие компьютерные преступления, подпадают под три категории: пираты, хакеры и кракеры

Рис. 2.14. Несанкционированный доступ к сетям и сетевым ресурсам

(взломщики). Пираты главным образом нарушают авторское право, создавая незаконные версии программ и данных. Хакеры получают неправомочный доступ к компьютерам других пользователей и файлам в них. Однако они, как правило, не повреждают и не копируют файлы, удовлетворяясь сознанием своей власти над системами. Кракеры позволяют себе все.

Обычно хакер проникает в систему по стандартной схеме. Сначала он определяет потенциально доступные компьютеры, затем пытается войти в систему и, если это удалось, старается закрепить свои позиции.

Первый этап процесса (обнаружение потенциально доступного компьютера) — самый простой. Сведения о них можно получить из файлов с расширением RHOSTS и .NETRS, содержащихся в уже взломанных системах, или с помощью доменной системы имен DNS (Domain Name System), которая является иерархической распределенной базой данных. Она обеспечивает преобразование имен компьютеров в числовые адреса сети Internet.

Одной из особенностей DNS, популярной среди хакеров, является так называемый запрос зонной информации (zone transfer). Когда сервер DNS получает подобный запрос, он передает всю имеющуюся информацию, относящуюся к зоне: имена компьютеров, их сетевые адреса и служебные данные о типе компьютера.

Имея эту информацию, хакер может составить точный список компьютеров, доступных для вмешательства. Например, из зонного информационного списка он может выбрать только компьютеры с операционной системой UNIX, использующие сетевое программное обеспечение BSD.

После того как хакер сделал свой выбор, перед ним встает задача входа в систему, то есть ее взлом. Большинство многопользовательских систем имеют средства идентификации пользователя. В системе UNIX идентифицируется традиционная пара: имя пользователя и пароль входа. Имена обычно известны, а пароли входа засекречены. Даже если имена пользователей неизвестны, их нетрудно получить, используя различные информационные утилиты. Что касается пароля входа, то перебор всех возможных вариантов, исходя из логических умозаключений, редко приводит к успеху: комбинаций слишком много, программа login работает медленно и обычно разъединяет линию связи после трех неудачных попыток. Для получения более эффективных результатов хакеры обращаются к сетевым средствам, которые предоставляют большинство систем.

После внедрения в систему хакер прежде всего пытается скрыть следы своего вмешательства путем изменения или удаления файлов-протоколов системы. Другим распространенным способом является обход ограничений удаленного входа с использованием средств дистанционного выполнения команд (REXEC). Эти средства позволяют пользователю выполнять команды на удаленном компьютере. При этом не остается записей в файлах протоколов, поэтому такой способ весьма популярен среди хакеров.

Общим методом незаметного внедрения в систему является использование средств удаленного выполнения команд для копирования файлов протоколов и дальнейшее проникновение в систему с помощью службы удаленного входа. Затем хакер пытается стать привилегированным пользователем и установить все файлы протоколов из копий, чтобы не оставлять следов своего пребывания в системе. Получение прав привилегированного пользователя никогда не было серьезной проблемой.

Проникнув в вычислительную систему, хакер закрепляет свое положение. Для этого может использоваться запись файлов .rhosts в домашние каталоги вскрытых пользователей или замена двоичных исполняемых файлов системы их подправленными вариантами. Он формирует такие файлы .rhosts, которые разрешают свободный доступ любому пользователю из любой системы.

Заменяя двоичные файлы, хакер может заменить команды su» и new-grp на специальные версии, которые предоставляют ему привилегированную операционную оболочку после указания специального пароля. Часто заменяются программы, запрашивающие пароли на вход. Эти программы продолжают работать как и обычные, но записывают введенные пароли в специальный файл, известный только хакеру.

Из практики известно, что как только хакеры становились привилегированными пользователями, они интересовались прежде всего почтовыми ящиками пользователей, файлами .rhosts и .netrc. Они определяли, кто является системным администратором, анализируя почтовые адреса или по принадлежности к специальной группе пользователей. Каталоги администраторов хакеры тщательно просматривали для выявления сообщений о недостатках и особенностях систем, а также поиска списков новых пользователей системы.

Раскрытие и модификация данных и программ

Раскрытие данных, хранящихся в оперативной памяти или программном обеспечении компьютеров вычислительных сетей, возможно в том случае, когда к ним имеет доступ практически любой пользователь сети. Кроме того, конфиденциальная информация может быть извлечена путем просмотра экрана монитора непосредственно или с использованием специальных приемных устройств на некотором расстоянии, а также из распечаток незашифрованных данных и документов (рис. 2.15).

Раскрытие данных угрожает сети, поскольку может иметь место следующее:

- некорректное управление доступом к данным со стороны администратора сети;
- неправильные установки управления доступом;
- незащищенность доступа к банкам данных и программному обеспечению;
- хранение данных в незашифрованном виде;
- установка мониторов и принтеров в незащищенных от посторонних лиц местах.

Одной из важнейших задач обеспечения сохранности информации в сети является организация надежной и эффективной системы архивации данных. В небольших сетях, где установлены один-два сервера, чаще всего применяется установка системы архивации непосредственно в свободные слоты серверов. В крупных корпоративных сетях предпочтительно выделить для архивации специализированный сервер.

Хранение архивной информации, представляющей особую ценность, должно быть организовано в специальном охраняемом помещении. Специалисты рекомендуют хранить дубликаты архивов наиболее ценных данных в другом здании на случай пожара или стихийного бедствия.

Рис. 2.15. Раскрытие и модификация данных и программ

Угроза модификации данных в файлах и программном обеспечении имеет место тогда, когда происходит их несанкционированное изменение (добавление, удаление и т. п.). Даже незначительная, на первый взгляд, модификация данных за достаточно продолжительный период времени может привести к существенному нарушению целостности всей имеющейся информации. А после несанкционированных изменений в командных файлах, сервисных и прикладных программах, а также заражения вирусами, как правило, данные при обработке искажаются и даже нарушается порядок доступа систем и служб к сети.

Наиболее распространенными уязвимыми местами систем являются:

- невозможность обнаружения изменений, вносимых в программное обеспечение;
- предоставление широкому кругу пользователей необоснованных полномочий доступа к информации, в том числе разрешение на запись;
- отсутствие средств выявления и защиты от вирусов;
- отсутствие криптографической контрольной суммы конфиденциальных данных.

Механизмы целостности данных и сообщений, предназначенные для защиты от угрозы несанкционированной модификации информации в компьютерных сетях, могут быть реализованы с помощью криптографических контрольных сумм и механизмов управления доступом и привилегий. При этом, как правило, применяемые в настоящее время механизмы целостности не могут предотвратить модификацию данных и сообщений, а позволяют ее только обнаружить.

В настоящее время в качестве криптографической контрольной суммы для обнаружения преднамеренной или случайной модификации данных используется код аутентификации сообщения — MAC (Message Authentication Code).

Принцип обнаружения модификации данных состоит в следующем. С помощью криптографического алгоритма и секретного ключа на основании содержания файла вычисляется начальное значение MAC, которое хранится в запоминающем устройстве. При необходимости проверки целостности файла производится повторный расчет MAC с использованием того же секретного ключа. В случае совпадения начального и повторного значений MAC принимается решение об отсутствии модификации файла.

Для обнаружения несанкционированных изменений в передаваемых сообщениях может быть применена электронно-цифровая подпись (ЭЦП). Суть работы системы ЭЦП заключается в следующем.

Для формирования ЭЦП используются криптографические алгоритмы с открытыми и секретными ключами. В криптографической системе с открытым ключом ЭЦП передаваемого сообщения формируется с помощью секретного ключа отправителя. Полученная ЭЦП и сообщение хранится в запоминающем устройстве или передается получателю. На приемной стороне ЭЦП может быть проверена с использованием общедоступного, открытого ключа создателя подписи. Если подпись однозначно идентифицирована, получатель принимает решение об отсутствии модификации принятого сообщения.

Кроме того, механизмы обеспечения целостности данных и сообщений могут играть важную роль для обнаружения вирусов, для строгого контроля над привилегиями пользователей и их правами доступа к ресурсам сети.

Данные механизмы могут быть реализованы с применением следующих средств и процедур защиты информации:

- использование кодов аутентификации сообщений;
- применение ЭЦП, основанной на криптографии с открытыми и секретными ключами;
- точное выполнение принятого механизма привилегий;
- назначение соответствующих прав пользователям для управления доступом;
- использование программ обнаружения вирусов;
- предотвращение локального хранения файлов и программного обеспечения.

Раскрытие, модификация и подмена трафика

Трафик — это поток данных, циркулирующих по передающей среде вычислительной сети. Раскрыть трафик можно путем подключения к кабельной линии передачи; перехвата информации, передаваемой по эфиру; подключением к сети сетевого анализатора и т. п. При этом оказывается возможным раскрытие паролей, системных имен и имен пользователей, сообщений электронной почты и других данных прикладного характера (рис. 2.16).

Эффективность воздействия такой угрозы на сетевой трафик возрастает в силу неадекватного внимания к защите информации. Например, пароли, которые хранятся в зашифрованном виде в системе, могут быть перехвачены при их пересылке в открытом виде от персонального компьютера к файловому серверу. А сообщения электронной почты, доступ к которым при хранении строго ограничен, зачастую пересылаются по линиям передачи компьютерной сети в открытом виде.

Рис. 2.16. Раскрытие, модификация и подмена трафика

Наиболее уязвимыми местами сети при раскрытии трафика являются:

- передача незашифрованных данных по каналам связи в сети;
- передача открытых данных с использованием общедоступных протоколов передачи;
- недостаточная физическая защита устройств и среды передачи.

В передающей среде сети могут происходить модификация или подмена трафика во время передачи, несмотря на то что данные, которыми обмениваются между собой пользователи сетей, не должны подвергаться несанкционированным изменениям.

В случае умышленного или случайного изменения любой части сообщения, включая адресную информацию как отправителя, так и получателя, имеет место модификацияданных.

Подмена трафика происходит тогда, когда злоумышленник маскируется под отправителя или получателя сообщений. Если он маскируется под отправителя, то заменяет адрес сообщения адресом истинного отправителя. При маскировке под отправителя злоумышленник подставляет свой адрес вместо истинного адреса получателя сообщения. В том и другом случаях предполагается перехват сообщений, циркулирующих между отправителем и получателем, а затем замена содержания сообщений. Эти действия злоумышленника получили название воспроизведениятрафика.

Для модификации или подмены трафика используют следующие уязвимые места:

- О отсутствие защиты трафика от воспроизведения;
- передача трафика в открытом виде;
- отсутствие в сообщениях отметки о дате и времени посылки;
- О отсутствие механизма аутентификации сообщения и цифровой подписи.

Проблемы защиты сети от перехвата пакетов сообщений

В настоящее время технология построения компьютерных сетей Ethernet стала самым распространенным решением обмена сообщениями между пользователями. Сети Ethernet завоевали огромную популярность благодаря высокой пропускной способности, простоте установки и приемлемой стоимости сетевого оборудования. Участки сетей, для которых скорости передачи данных 10 Мбит/с недостаточно, можно довольно легко модернизировать, чтобы повысить скорость до 100 Мбит/с (Fast Ethernet) или даже до 1 Гбит/с (Gigabit Ethernet).

Однако технология Ethernet не лишена существенных недостатков. Основной из них — передаваемая информация не защищена. Компьютеры, подключенные к сети Ethernet, оказываются в состоянии перехватывать информацию, адресованную своим соседям. Основная причина — принятый в сетях Ethernet так называемый широковещательный механизм обмена сообщениями.

В сети типа Ethernet подключенные к ней компьютеры, как правило, совместно используют один и тот же кабель, который служит средой для пересылки сообщений между ними.

Известно, что если в комнате одновременно громко говорят несколько людей, разобрать что-либо из сказанного ими будет очень трудно. Так происходит и в Ethernet. Когда по сети начинают «общаться» сразу несколько компьютеров, выделить из их «цифрового гвалта» полезную информацию и понять, кому именно она предназначена, практически невозможно. В отличие от человека, компьютер не может поднять руку и попросить тишины, поэтому для решения данной проблемы требуются иные, более сложные действия.

Компьютер сети Ethernet, желающий передать какое-либо сообщение по общему каналу, должен удостовериться, что этот канал в данный момент свободен. В начале передачи компьютер прослушивает несущую частоту сигнала, определяя, не произошло ли искажения сигнала в результате возникновения коллизий с другими компьютерами, которые ведут передачу одновременно с ним. При наличии коллизии компьютер прерывает передачу и «замолкает». По истечении некоторого случайного периода времени он пытается повторить передачу.

Если компьютер, подключенный к сети Ethernet, ничего не передает сам, он, тем не менее, продолжает «слушать» все сообщения, передаваемые по сети. Заметив в заголовке поступившей порции данных свой сетевой адрес, компьютер копирует эти данные в собственную локальную память.

Существуют два основных способа объединения компьютеров в сеть Ethernet.

В первом случае компьютеры соединяются при помощи коаксиального кабеля. Этот кабель черной змейкой вьется от компьютера к компьютеру, соединяясь с сетевыми адаптерами Т-образным разъемом. Такая топология на языке профессионалов называется сетью Ethernet 10Base2. Однако ее еще можно назвать сетью, в которой «все слышат всех». Любой компьютер, подключенный к сети, способен перехватывать данные, посылаемые по этой сети другим компьютером.

Во втором случае каждый компьютер соединен кабелем типа витая пара с отдельным портом центрального коммутирующего устройства — концентратора или коммутатора. В таких сетях, которые называются сетями Ethernet JOBaseT, компьютеры поделены на группы, именуемые доменами коллизий. Домены коллизий определяются портами концентратора или коммутатора, замкнутыми на общую шину. В результате коллизии возникают не между всеми компьютерами сети, а между теми из них, которые входят в один и тот же домен коллизий. За счет этого повышается пропускная способность всей сети.

В последнее время в крупных сетях стали появляться коммутаторы нового типа, которые не используют широковещание и не замыкают группы портов между собой. Вместо этого все передаваемые по сети данные буферизуются (накапливаются) в памяти и затем отправляются по мере возможности. Однако подобных сетей пока довольно мало — не более 10% от общего числа сетей типа Ethernet.

Таким образом, принятый в подавляющем большинстве Ethernet-сетей алгоритм передачи данных требует, чтобы каждый компьютер, подключенный к сети, непрерывного «прослушивал» весь без исключения сетевой трафик. Предложенные алгоритмы, при использовании которых компьютеры отключались бы от сети во время передачи «чужих» сообщений, так и остались нереализованными из-за их чрезмерной сложности и малой эффективности.

Как уже было сказано, сетевой адаптер каждого компьютера в сети Ethernet, как правило, «слышит» все, о чем «толкуют» между собой его соседи по сегменту этой сети. Но обрабатывает и помещает в свою локальную память он только те порции данных (так называемые кадры), которые содержат его уникальный сетевой адрес.

В дополнение к этому подавляющее большинство современных Ethernet-адаптеров допускают функционирование в особом режиме, называемом беспорядочным (promiscuous). При использовании данного режима адаптер копирует в локальную память компьютера все без исключения передаваемые по сети кадры данных.

Специализированные программы, переводящие сетевой адаптер в беспорядочный режим и собирающие весь трафик сети для последующего анализа, называются анализаторами протоколов или снифферами. Администраторы сетей широко применяют анализаторы протоколов для контроля за работой этих сетей и определения их перегруженных участков, отрицательно влияющих на скорость передачи данных. К сожалению, анализаторы протоколов используются и злоумышленниками, которые с их помощью могут перехватывать чужие пароли и другую конфиденциальную информацию.

Надо отметить, что анализаторы протоколов представляют серьезную опасность. Само присутствие в компьютерной сети анализатора протоколов указывает на то, что в ее защите имеется брешь. Установить анализатор протоколов мог посторонний человек, который проник в сеть извне (например, если сеть имеет выход в Internet). Но это могло быть и делом рук доморощенного злоумышленника, имеющего легальный доступ к сети. В любом случае к сложившейся ситуации нужно отнестись со всей серьезностью.

Специалисты в области компьютерной безопасности относят атаки на компьютеры при помощи анализаторов протоколов к так называемым атакам второго уровня. Это означает, что компьютерный взломщик уже сумел проникнуть сквозь защитные барьеры сети и теперь стремится развить свой успех. При помощи анализатора протоколов он может попытаться перехватить регистрационные имена и пароли пользовате-

лей, их секретные финансовые данные (например, номера кредитных карточек) и конфиденциальные сообщения (к примеру, электронную почту). Имея в своем распоряжении достаточные ресурсы, компьютерный взломщик в принципе может перехватывать всю информацию, передаваемую по сети.

Анализаторы протоколов существуют для любой платформы. Но даже если окажется, что для какой-то платформы анализатор протоколов пока еще не написан, с угрозой, которую представляет атака на компьютерную систему при помощи анализатора протоколов, по-прежнему приходится считаться. Дело в том, что анализаторы протоколов исследуют не конкретный компьютер, а протоколы. Поэтому анализатор протоколов может обосноваться в любом узле сети и оттуда перехватывать сетевой трафик, который в результате широковещательных передач попадает в каждый компьютер, подключенный к сети.

Одна из первых атак, проведенных при помощи анализаторов протоколов, была зафиксирована в 1994 году в США. Тогда неизвестный злоумышленник разместил анализатор протоколов на различных хостах и магистральных узлах сетей Internet и Milnet, в результате чего ему удалось перехватить более 100тыс. регистрационных имен и паролей пользователей. Среди пострадавших от атаки оказались Калифорнийский государственный университет и Ракетная лаборатория министерства обороны США.

Наиболее частыми целями атак компьютерных взломщиков, осуществляемых с использованием анализаторов протоколов, становятся университеты. Хотя бы из-за огромного количества различных регистрационных имен и паролей, которые могут быть украдены в ходе такой атаки. Да и сами студенты отнюдь не брезгуют возможностями анализаторов протоколов. Нередкий случай, когда несколько студентов, заняв компьютер, подключенный к локальной сети университетской библиотеки, быстро устанавливают с нескольких дискет анализатор протоколов. Затем они просят ничего не подозревающую жертву, сидящую за соседним компьютером: «Вы не могли бы заглянуть в свой почтовый ящик, а то у нас почему-то электронная почта не работает?». Несколько минут спустя вся эта группа компьютерных взломщиков-любителей, перехватив регистрационное имя и пароль доступа соседа к почтовому серверу, с удовольствием знакомится с содержимым его почтового ящика и посылает письма от его имени.

Использование анализатора протоколов на практике не является такой уж легкой задачей, как это может показаться. Чтобы добиться от него хоть какой-то пользы, компьютерный взломщик должен хорошо знать сетевые технологии. Просто установить и запустить анализатор протоколов нельзя, поскольку даже в небольшой локальной сети из пяти компьютеров трафик составляет тысячи и тысячи пакетов в час. Следовательно, за короткое время выходные данные анализатора протоколов заполнят весь жесткий диск.

Компьютерный взломщик, как правило, настраивает анализатор протоколов так, чтобы он перехватывал только первые 200—300 байт каждого пакета, передаваемого по сети. Обычно именно в заголовке пакета размещается информация о регистрационном имени и пароле пользователя, которые и интересуют взломщика. Тем не менее, если в распоряжении взломщика имеется достаточно пространства на жестком диске, то увеличение объема перехватываемого графика пойдет ему только на пользу. В результате он может дополнительно узнать много интересного.

На серверах в сети Internet есть множество анализаторов протоколов, которые отличаются лишь набором доступных функций. В настоящее время получили распространение 2 вида анализаторов:

- пассивные;
- активные.

Различие их состоит в том, что пассивные снифферы не производят модификацию перехватываемых пакетов.

В качестве интерфейса пассивный сниффер может использовать либо сетевую плату компьютера, либо модемное подключение к Internet. В случае подключения через модем утилита позволяет просматривать пакеты, адресованные только вашему компьютеру. При использовании сетевой платы компьютера сниффер переводит сетевой адаптер в режим перехвата всех пакетов из сегмента, в котором находятся компьютер и сниффер.

Поскольку в сети постоянно циркулирует огромное количество пакетов, их необходимо отфильтровывать. Первый критерий фильтрации — глобальный: все кадры Ethernet без разбора или только IP. Кроме того, фильтр позволяет отбирать трафик SNMP и SNA. В зарегистрированной версии прием пакетов можно также ограничить только уникальными, групповыми, широковещательными адресами или любой их комбинацией. Пассивный сниффер ориентирован прежде всего на IP, поэтому дальнейшей фильтрации подвергается именно трафик IP. Пользователь может выбрать тип протокола третьего и четвертого уровней (TCP, VDP, IGMP — всего полтора десятка) и порт. Порт задается «в лоб» с помощью номера, который можно выбрать из списка. Самые распространенные — HTTP, FTP, POP3, Telnet и т. п.

Точная настройка состоит в возможности отбора пакетов по IP-адресам отправителя и получателя (направление передачи имеет значение) или по ключевым словам. Различные настройки фильтра можно сохранять в файлах и задействовать в определенных ситуациях. Фильтрация пакетов не только ограничивает собираемую снифферером информацию, но и обеспечивает его нормальную работу.

Задание слишком большого числа вариантов для IP приводит к тому, что пассивный сниффер иногда не успевает обрабатывать часть пакетов.

Собранные пакеты отображаются в окне снифферa в виде списка с указанием MAC-адресов получателей и отправителей, типа пакета, типа протокола, IP-адресов и номеров портов. Содержимое любого пакета можно просмотреть в виде шестнадцатеричного кода и текста. Это не всегда удобно, поэтому собранную информацию можно сохранить в виде файла и обработать с помощью специальной утилиты, которая сортирует пакеты по адресам и представляет их содержимое в удобочитаемом виде.

Подобные снифферы не рассчитаны на работу в больших сетях, поскольку их производительность ограничена. Тем не менее, эти программы позволяют анализировать события, происходящие в небольшой сети (точнее, в ее конкретном сегменте), разумеется, при наличии соответствующих познаний, так как аналитические функции отсутствуют. Чтобы обнаружить избыток пакетов какого-либо типа, их надо уметь опознавать. Впрочем, все основные сервисы IP вполне успешно распознаются, а уже одного этого кому-то будет вполне достаточно.

Для выявления снифферов в программном обеспечении компьютера следует использовать то обстоятельство, что заложенная хакерская программа периодически сбрасывает накопленную информацию в один из почтовых ящиков, зарегистрированных на бесплатном сервере электронной почты.

Вредоносное программное обеспечение

Вредоносное программное обеспечение — это любая программа, написанная с целью нанесения ущерба или использования ресурсов атакуемого компьютера. Вредоносное программное обеспечение часто скрыто внутри обычных программ или замаскировано под них. В некоторых случаях оно само тиражируется на другие компьютеры по электронной почте или через инфицированные дискеты и CD. Одними из основных характеристик современных вирусных атак являются высокая скорость их распространения и частота появления новых атак.

О вредоносном программном обеспечении, подстерегающем доверчивых пользователей, широкая публика наслышана больше, чем о каких-либо других опасностях и повреждениях компьютерной техники. Это вирусы, черви, троянские кони, логические бомбы, зомби, программные закладки, модули считывания паролей — список можно продолжить. Вредоносное программное обеспечение различных типов использует весьма разнообразные методы воздействия на информацию, степень опасности такого рода программ тоже различна.

Бурное развитие информационных технологий привело к налаживанию международных связей, в том числе и межконтинентальных, к становлению внутри- и межгосударственных потоков информации, измеряемыми многими десятками терабайт в секунду.

Анализ развития компьютеризации на мировом уровне показывает, что число пользователей достигло 350 млн, начав свой отсчет практически от нулевой отметки в 1981 году.

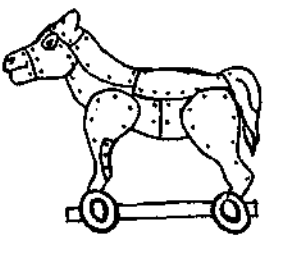
В период с 1998 по 1999 год произошло резкое увеличение числа компьютерных атак, хотя около 98% всех пользователей применяли доступные средства защиты. Объяснить эту тенденцию можно тем, что Internet превратился в хорошо организованную систему с унифицированным программным обеспечением. Тем самым пользователи сети стали во многом зависеть от качества программного обеспечения, которое они используют для работы.

Рост числа несанкционированных проникновений в информационные ресурсы лучше всего прослеживается путем анализа взаимосвязи частоты инцидентов, с одной стороны, и уязвимостью программного обеспечения — с другой.

Инцидент — это группа атак, объединенных по таким характерным признакам, как время проведения атаки, средства атакующих, цель нападения и т. д.

Под термином уязвимость имеется в виду слабое место в программном обеспечении, которое может быть использовано злоумышленником в своих целях. Уязвимость программного обеспечения, как правило, обусловлена следующими ошибками:

- в программном обеспечении (уязвимость реализации);
- в конфигурации программного обеспечения (уязвимость конфигурации);
- не связанными напрямую с конкретным программным обеспечением (уязвимость проектирования).



Количество уязвимых мест в программном обеспечении во многом определяется степенью популярности продукта. В принципе, чем популярнее система и чем больше пользо-

вателей отдают ей предпочтение, тем сильнее стремление злоумышленников организовать атаку именно на эту систему.

Другой фактор, способствующий увеличению количества атак за последние годы, — резкое понижение требований к квалификации атакующего. Это объясняется тем, что большинство современных программ, реализующих ту или иную атаку, доступны в настоящий момент в Internet и, как правило, имеют простой и дружелюбный пользовательский интерфейс. Атакующему необходимо ввести лишь DNS-имя или IP-адрес компьютера-жертвы и нажать кнопку. При этом не требуется, чтобы злоумышленник имел представление о принципах работы механизмов, с помощью которых осуществляется атака.

Если во второй половине 80-х годов к наиболее популярным средствам атакующих относилось использование известных паролей и уже раскрытых уязвимых мест в системе безопасности, то сегодня к этому добавились средства, использующие недостатки в протоколах, средства анализа исходных текстов программ для выявления новых уязвимых мест, установка программ-анализаторов сетевого трафика, подмена IP-адреса источника нападения, атаки типа «отказ в обслуживании», средства автоматизированного сканирования сети, распределенные атаки и многие другие.

Суммарный ущерб от компьютерных атак в период с 1997 по 2000 год только в США составил 626 млн долларов. Эти цифры позволяют говорить о том, что криминальная прослойка в «информационном обществе» состоялась и что обществу противостоит организованная преступность.

Миллионы людей путешествуют по сети, «перехватывая» то тут, то там разнообразные программы и другую полезную информацию. После чего они немедленно «опробуются в деле», ну а дальше... кому как повезет. В сети находятся гигабайты информации и неизвестно, сколько в ней вирусов (случайно попавших или намеренно «подсаженных»). И при этом приходится только удивляться беспечности тех, кто тщательно проверяет все «внешние» дискеты и диски, но даже и не задумывается, что вирусы могут присутствовать в программе и в документе, полученных из сети.

Еще не так давно вирусы распространялись только через дискеты. Они назывались вирусами загрузочного сектора, потому что попадали в компьютер с дисковода для гибких дисков. Тогда вирусная инфекция распространялась достаточно ограниченно и требовала намного больше времени, чем сейчас. Затем появились приложения типа Microsoft Outlook или Word, использующие макросы, что привело к возникновению множества макровирусов. Были созданы вирусы Мелисса, Чернобыль, программа Worm.Explore.Zip и другие вирусы массовой рассылки, распространявшиеся по электронной почте. Эти программы нанесли серьезный ущерб персональным компьютерам во всех странах мира.

На пользователей обрушился вирус, получивший название BubleBoy, которым можно заразить компьютер, всего лишь открыв свою электронную почту, поскольку он использовал язык описания сценариев Visual Basic. Вирусы по-прежнему остаются самой серьезной проблемой компьютерной защиты.

К середине 2001 года ущерб, нанесенный компьютерными вирусами, измеряется в 10,7 млрд долларов против 17,1 млрд в 2000 году и 12,1 млрд в 1999 году. По данным аналитиков, ущерб, нанесенный вирусом Code Red, оценивается в 2,6 млрд долларов, причем на работы по восстановлению компьютеров потрачено 1,1 млрд долларов, а на

компенсацию производственных потерь — 1,5 млрд долларов. Вирус Sircam нанес ущерб в размере 1,035 млрд долларов, а вирус Love Bug — 8,7 млрд долларов. И потери от них продолжают расти, а ведь здесь перечислены лишь некоторые из распространенных вирусов.

Атаки на отказ от обслуживания обрушиваются на крупнейшие Web-узлы электронной коммерции. Они тоже инициированы вредоносным программным обеспечением, проникшим в сотни компьютеров, подключенных к Internet, причем владельцы этих систем о том и не подозревали.

Небольшие организации, специалисты и добровольцы предпринимают активные действия, чтобы каталогизировать вредоносное программное обеспечение, рассылают предупреждения и предлагают программное обеспечение, способное выявлять такие программы, определять их местонахождение и уничтожать. Новые вредоносные программы появляются каждый месяц, они создаются подпольными группами программистов, стремящихся испортить или украсть информацию, а иногда просто продемонстрировать свое техническое мастерство.

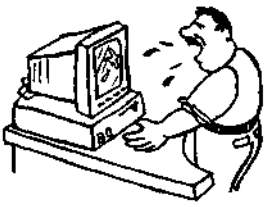
Рассмотрим более подробно, что же собой представляет вредоносное программное обеспечение и как оно себя проявляет.

Вирусы

Компьютерные вирусы — известный всем вид вредоносного программного обеспечения. Это программы, обладающие способностью к самовоспроизведению (размножению) в среде стандартной операционной системы путем включения в исполняемые или хранящиеся программы своей, возможно, модифицированной копии, способной к дальнейшему размножению. Указанное свойство присуще всем типам компьютерных вирусов. Кроме того, термин «способность к самовоспроизведению» надо трактовать широко. Различные экземпляры одного вируса не только не обязаны полностью совпадать, но могут даже не иметь ни одного одинакового байта (речь идет о так называемых полиморфных вирусах).

Свойство размножения вирусов само по себе, в принципе, не представляет опасности; размножение вирусов может привести, в основном, к заполнению пространства свободной памяти, увеличению хранящихся файлов и замедлению выполнения программ.

Но если подобный вирус начнет размножаться по сети, то в один прекрасный день эта сеть может быть полностью заблокирована. Например, в середине января 1999 года в сети Internet был обнаружен компьютерный червь, получивший прозвище Happy99.exe. Он не пытается разрушать файлы на зараженных компьютерах, зато без ведома жертвы рассылает электронные письма и объявления для телеконференций и способен не только снизить производительность сети, но даже вывести из строя корпоративный сервер электронной почты.



От опасного вируса CIH (Чернобыль), который активировался 26 апреля 1999 года, в день тринадцатой годовщины катастрофы на Чернобыльской АЭС, пострадало более 100тыс. компьютеров только в России. По прогнозам Е. Касперского, руководителя антивирусного центра «Лаборатория

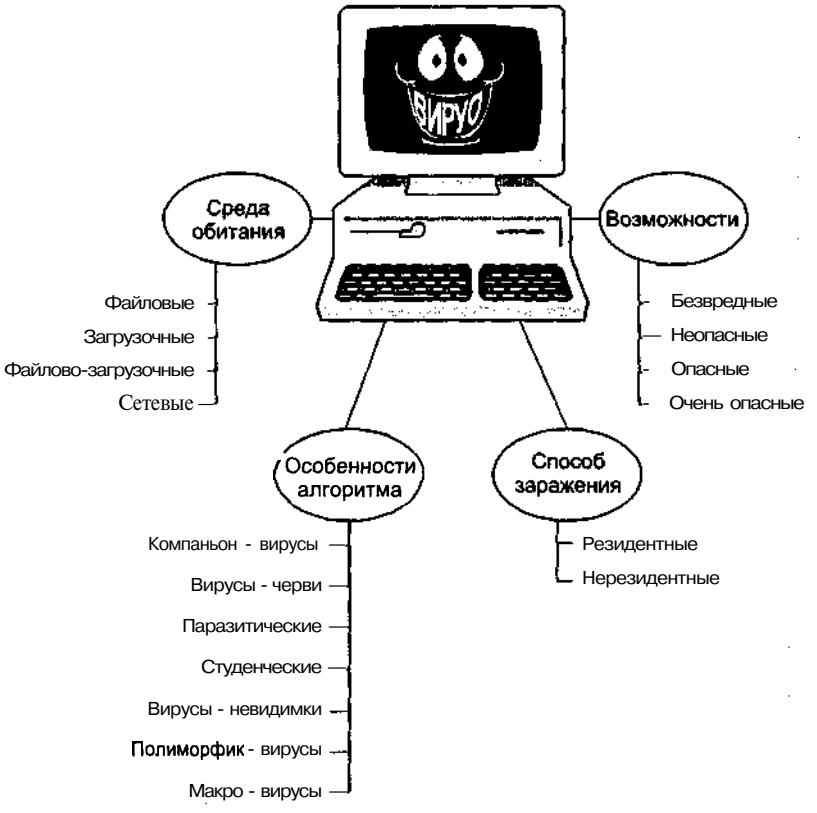


Рис. 2.17. Классификация компьютерных вирусов

Касперского», основные причины распространения вируса — нелегальное зараженное программное обеспечение.

Сами механизмы воспроизведения вирусов тоже могут быть весьма разнообразны. Эти программы незаметно присоединяются к другим исполняемым модулям. Они опасны тем, что, прежде чем нанести вред, на который они и запрограммированы, копируют себя в другие программные файлы. Таким образом, компьютерные вирусы заражают и воспроизводятся аналогично биологическим.

Считается, что сам термин «компьютерный вирус» впервые употребил сотрудник Лехайского университета (США) Ф. Коэн на конференции по безопасности информации в 1984 году. Прошли годы. И что же сегодня представляют собой компьютерные вирусы?

Существует формальная система, позволяющая классифицировать компьютерные вирусы и называть их так, чтобы избежать ситуации, когда один и тот же вирус имеет неузнаваемо разные имена в классификации разных разработчиков антивирусных программ. Однако еще нельзя говорить о полной унификации имен и характеристик вирусов.

Мы будем исходить из того, что обычному пользователю нет необходимости вникать во все тонкости функционирования вируса: объекты атаки, способы заражения, осо-

бенности проявления и пр. Но желательно знать, какими бывают вирусы, понимать общую схему их работы. Условно компьютерные вирусы можно подразделить на классы (рис. 2.17). Эта классификация объединяет, естественно, далеко не все возможные вирусы; в каждой категории встречаются экзотические варианты, которые не названы.

Жизненный цикл компьютерного вируса может включать следующие этапы:

- внедрение (инфицирование);
- инкубационный период;
- саморазмножение (репродуцирование);
- выполнение специальных функций;
- проявление.

Данные этапы не являются обязательными и могут иметь другую последовательность. Особую опасность представляет этап выполнения специальных функций, которые могут привести к катастрофическим последствиям.

Компьютерные вирусы могут неограниченное время храниться на дискетах и жестких дисках, а затем случайно или умышленно инфицировать компьютер при использовании зараженных файлов.

Вирус проникает в компьютер только при выполнении зараженной программы. Но если компьютер уже заражен, то практически любая операция на нем может привести к заражению программ и файлов, находящихся в памяти и на дискетах, вставленных в дисковод.

При наличии в памяти компьютера программы с телом вируса могут заражаться как выполняемые программы, так и хранящиеся на жестком диске и дискетах, а также файлы на дискетах при просмотре их каталогов, то есть происходит внедрение вируса.

Копия вируса вставляется в зараженную программу таким образом, чтобы при запуске зараженной программы вирус получил управление в первую очередь. Первым и обязательным действием вируса при выполнении инфицированной программы является саморазмножение. Этот этап может длиться вплоть до уничтожения вирусоносителя. Одновременно с внедрением или после некоторого промежутка времени определенного числа внедренных копий и т. д. вирус приступает к выполнению специальных функций, именуемых еще логическими бомбами, которые вводятся в программное обеспечение и срабатывают только при выполнении определенных условий, например, по совокупности даты и времени, и частично или полностью выводят из строя компьютерную систему.

Не следует думать, что логические бомбы — это экзотика, не свойственная нашему обществу. Логическая бомба, которая срабатывает по достижении определенного момента времени, получила названия временной бомбы. Она «взрывается» неожиданно, разрушая данные.

Кроме того, часть компьютерных вирусов имеет фазу проявления, которая сопровождается визуальными или звуковыми эффектами. Отдельные вирусы сообщают пользователю о заражении компьютера.

Существует способ внедрения в чужое программное обеспечение, именуемый троянским конем (Trojan Horse). Конечно, нельзя узнать, что думали жители Трои на другой день после того, как с радостными криками и песнями вкатили в город огромного деревянного коня — «подарок» от якобы побежденных ахейцев. Так же трудно порой бывает восстановить работоспособность компьютера, по «программному полю»

которого «проскачут» такие кони. Действие программ-диверсантов заключается в тайном введении в атакуемую программу команд, выполняющих функции, не планируемые владельцем программы, но при этом сохранять и прежнюю работоспособность программы.

С помощью троянских программ преступники, например, отчисляют на свой счет определенную сумму с каждой банковской операции. В США получила распространение такая форма компьютерного вандализма, когда «троянский конь» разрушает через какое-то время все программы, хранящиеся в памяти компьютера.

Компьютерные программные тексты обычно чрезвычайно сложны. Они состоят из сотен, тысяч, а иногда и миллионов команд. Поэтому «троянский конь» из нескольких десятков команд вряд ли будет обнаружен, если, конечно, нет подозрений относительно его существования в программе, но даже и, предполагая его наличие, экспертам-программистам потребуется много дней и недель, чтобы найти троянца.

Есть еще одна разновидность «троянского коня». Ее особенность состоит в том, что в безобидно выглядящий кусок программы вставляются не команды, выполняющие «грязную» разрушительную работу, а команды, формирующие такие команды и после выполнения их уничтожающие. В этом случае программисту, пытающемуся найти «троянского коня», необходимо искать не его самого, а команды, его формирующие. Развивая эту идею, можно представить себе команды, которые создают другие команды и т. д. (сколь угодно раз), а в итоге, создающие «троянского коня».

Современная техническая литература, посвященная проблемам компьютерных вирусов, изобилует различными терминами, заимствованными из других отраслей науки и научно-фантастических книг, поэтому очень часто одни и те же вирусы имеют разное название.

Все известные вирусы можно разделить на классы по следующим признакам:

- ❑ среда обитания;
- О способ заражения среды обитания;
- О деструктивная возможность;
- ❑ особенности алгоритма вируса.

По среде обитания компьютерные вирусы можно разделить на загрузочные, файловые, файлово-загрузочные и сетевые.

Загрузочные (бутовые) вирусы внедряются в загрузочный сектор диска (boot-сектор) или в сектор, содержащий системный загрузчик винчестера (Master Boot Record). Часто эти вирусы «всеядны»: они заражают и то, и другое.

Файловые вирусы — в простейшем случае такие вирусы, которые заражают исполняемые файлы. Если с загрузочными вирусами все более или менее ясно, то файловые вирусы — это гораздо менее определенное понятие. Достаточно, к примеру, сказать, что файловый вирус может вообще не модифицировать файл (вирусы-спутники и вирусы семейства Dir). Кроме того, к файловым относятся так называемые macro-вирусы. О них мы еще поговорим.

Помимо этого, существуют и их сочетания — например, файлово-загрузочные вирусы, заражающие файлы и загрузочные сектора дисков. Такие вирусы, как правило, работают по довольно сложным алгоритмам и часто применяют оригинальные методы проникновения в систему. Вирусов этого типа не очень много, но среди них встречаются чрезвычайно злобные экземпляры (например, известный вирус OneHalf).

Сетевые вирусы распространяются по компьютерной сети, заражая сотни и тысячи компьютеров. Варианты заражения вирусами представлены на рис. 2.18.

Вирусы могут размешаться в следующих системах и структурах:

- О операционной системе, где они «сцепляются» с программами, расположенными в системной части дискеты или жесткого диска;
- ❑ библиотеках компиляторов для внедрения в программы, составляемые компиляторами;
- ❑ сетевых драйверах;
- ❑ «плохих» или специальных секторах жесткого диска;
- ❑ ПЗУ в качестве программно-технической закладки;
- ❑ структуре исполняемых программ или файловых программ.

Способ заражения среды обитания подразделяется на резидентный и нерезидентный.

Резидентный вирус при инфицировании компьютера оставляет в оперативной памяти свою резидентную часть, которая затем перехватывает обращение операционной системы к объектам заражения и внедряется в них. Происходит это следующим образом: резидентный вирус запрашивает у системы участок памяти и копирует себя в него. Он перехватывает прерывания, анализирует их и обеспечивает тем самым управление процессором компьютера. Если следующим этапом жизненного цикла вируса является инкубационный период, то вирус никак не проявляет себя в течение определенного промежутка времени или до достижения определенного числа подходящих объектов заражения. После этого наступает этап размножения. Обнаружив обращение к компонентам системы, пригодным для заражения, вирус активизирует процедуру копирования. Обычно эта процедура предусматривает проверку, не присутствует ли уже в объекте копия вируса (если копия присутствует, то объект уже заражен); отдельные вирусы проверяют номер версии и заражают объект, если их версия более новая. Если копии вируса нет, то он копируется из памяти в заражаемый объект с модификацией его первой команды. Объектами заражения в этом случае могут быть исполняемые программы на жестком диске и дискетах. Резидентные вирусы находятся в памяти и активны вплоть до выключения или перезагрузки компьютера.

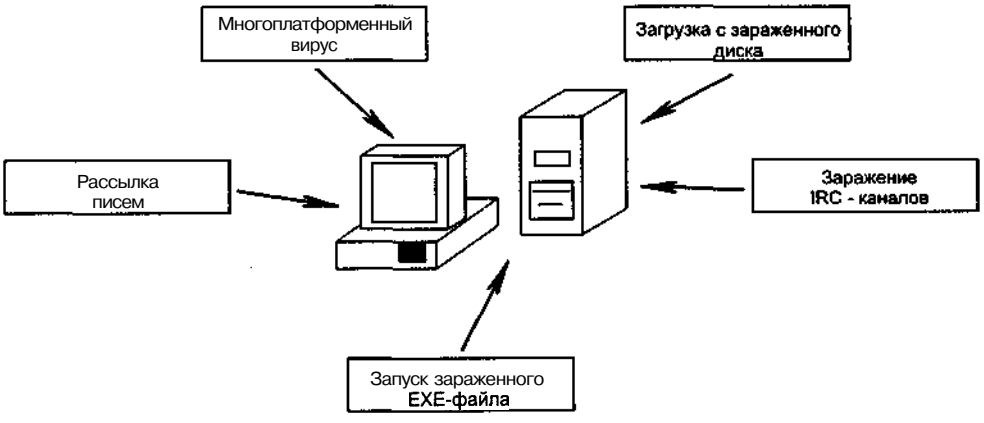


Рис. 2.18. Варианты заражения вирусами

Нерезидентные (транзитные) вирусы не заражают память компьютера и активны ограниченное время. Некоторые вирусы оставляют в оперативной памяти небольшие резидентные программы, которые не распространяют вирус. Такие вирусы тоже считаются нерезидентными.

Транзитные вирусы не остаются в памяти после выполнения зараженной программы. В этом случае вирус перед передачей управления исходной программе ищет еще не зараженный файл, пригодный для внедрения. Тогда выполнение специальных функций не всегда следует за этапом саморазмножения, чтобы успеть создать достаточное количество своих копий, прежде чем факт заражения будет обнаружен. Поэтому механизм выполнения специальных функций включается достаточно редко и вредные последствия вируса сначала могут быть незаметны. Когда же пользователь заметит изменения в работе компьютера, может оказаться, что вирусом поражены практически все файлы системы.

По деструктивным способностям вирусы можно разделить на:

- безвредные;
- неопасные;
- опасные;
- очень опасные.

Безвредные вирусы только уменьшают объем свободной памяти на диске в результате своего распространения, а больше никак не влияют на работу компьютера.

Влияние неопасных вирусов ограничивается также уменьшением свободной памяти на диске и дополнительно сопровождается графическими, звуковыми и другими эффектами.

Опасные вирусы приводят к серьезным сбоям в работе компьютера.

В результате работы очень опасных вирусов уничтожаются программы, данные, удаляется необходимая для работы компьютера информация, записанная в системных областях памяти. Особо опасны вирусы, прикрепляемые к объектной библиотеке какого-либо компилятора. Такие вирусы автоматически внедряются в любую программу, работающую с инфицированной библиотекой.

Известные в настоящее время вирусы могут выполнять следующие разрушительные функции:

- изменение данных в файлах;
- изменение данных, передаваемых через параллельные и последовательные порты;
- изменение назначенного диска (запись информации производится не на диск, указанный пользователем, а на диск, указанный вирусом);
- переименование файлов (не сообщая об этом пользователю);
- форматирование отдельных частей жесткого диска (дискеты) или даже всего диска (дискеты);
- уничтожение каталога диска;
- нарушение работоспособности операционной системы, в результате чего она не воспринимает внешних воздействий пользователя и требует перегрузку;
- снижение производительности из-за постоянного выполнения паразитных программ;
- отказ в выполнении определенной функции (например, блокировка клавиатуры, блокировка загрузки программы с защищенной от записи дискеты и т. д.);
- стирание информации, выводимой на экран дисплея и т. п.;

- «мелкие» повреждения данных (например, замена первых байтов каждого блока при записи, замена отдельных символов и т. д.), которые пользователь долго не может обнаружить.

Перечень специальных функций, выполняемых вирусами, практически пополняется с каждым новым видом вируса. Исследователи различают множество видов вирусов, по механизмам размножения и выполняемым специальным функциям. Среди этих видов существует много вариаций (штаммов), которые являются, как правило, результатом усовершенствования одним программистом вируса, созданного другим. Обычно легче модифицировать чужую программу, чем создать оригинальную собственную.

Но даже если в алгоритме вируса не найдено ветвей, наносящих ущерб системе, этот вирус нельзя с полной уверенностью назвать безвредным, так как проникновение его в компьютер может вызвать непредсказуемые, а порой и катастрофические, последствия. Ведь в вирусе, как и во всякой программе, встречаются ошибки, в результате которых могут быть испорчены как файлы, так и сектора дисков. Возможно также «заклинивание» резидентного вируса и системы при работе в новых версиях DOS, в Windows или в других мощных системах.

По особенностям алгоритма функционирования вирусов их можно подразделить на следующие группы:

- компаньон-вирусы (companion);
- вирусы-черви (worm);
- паразитические;
- студенческие;
- stealth-вирусы (вирусы-невидимки);
- полиморфик-вирусы (polymorphic);
- макро-вирусы.

Компаньон-вирусы (companion) представляют собой программы, не изменяющие файлы. Эти вирусы создают для EXE-файлов, находящихся в памяти компьютера, файлы-спутники, имеющие то же самое имя, но с расширением COM, например, для файла XCOPY.EXE создается файл XCOPY.COM. Вирус записывается в COM-файл и никак не изменяет EXE-файл. При запуске такого файла DOS первым обнаружит и выполнит COM -файл, то есть вирус, который затем запустит и EXE -файл.

Вирусы-черви распространяются в компьютерных сетях. Они, как и компаньон-вирусы, не изменяют файлы или секторы на дисках. Они проникают в память компьютера из компьютерной сети, вычисляют сетевые адреса других компьютеров и рассылают по этим адресам свои копии. Такие вирусы иногда создают рабочие файлы на дисках системы, но могут вообще не обращаться к ресурсам компьютера (за исключением оперативной памяти).

Паразитические вирусы при распространении своих копий обязательно изменяют содержимое дисковых секторов или файлов. К этой группе относятся все вирусы, которые не являются вирусами-червями или компаньон-вирусами.

Студенческие вирусы — это крайне примитивные вирусы, часто нерезидентные и содержащие большое число ошибок.

Stealth-вирусы, или вирусы-невидимки, представляют собой весьма совершенные программы, которые перехватывают обращения DOS к пораженным файлам или сек-

торам дисков и «подставляют» вместо себя незараженные участки информации. Кроме этого, такие вирусы при обращении к файлам используют достаточно оригинальные алгоритмы, позволяющие обманывать резидентные антивирусные программы.

Способов маскировки вирусов существует великое множество, но все они основаны на перехвате вирусами прерываний BIOS и операционной системы. Перехватив прерывания, вирусы контролируют доступ к зараженным объектам. Например, при просмотре зараженного объекта они могут «подсунуть» вместо него здоровый. Кроме того, вирусы искажают информацию DOS (например, возвращают неверное значения длины файла, скрывая свое присутствие в нем). Для большинства антивирусных программ вирусы, использующие стелс-технологию, являются серьезной проблемой.

Полиморфик-вирусы — это достаточно трудно обнаруживаемые вирусы, не имеющие сигнатур, то есть не содержащие ни одного постоянного участка кода. В большинстве случаев два образца одного и того же полиморфик-вируса не будут иметь ни одного совпадения. Это достигается шифрованием основного тела вируса и модификациями программы-расшифровщика.

Вирусы, шифрующие свой код, известны довольно давно. Однако сами процедуры дешифрования достаточно легко выявить, в частности, потому, что далеко не все авторы вирусов имеют достаточно знаний для написания собственных процедур шифрования и дешифрования, поэтому многие вирусы используют для этих целей один и тот же код. Теперь сканеры вирусов ищут определенные процедуры дешифрования. Хотя обнаружение такой процедуры еще ничего не говорит о том, какой именно вирус присутствует в зашифрованном виде, но уже сигнализирует о наличии вируса.

Поэтому последней уловкой злоумышленников становится полиморфизм. В прежние времена обнаружение вирусов было простым делом: каждый вирус создавал точную копию самого себя при тиражировании и инфицировании новых файлов и загрузочных секторов, поэтому антивирусным программам требовалось только знать последовательность байтов, составляющих вирус. Для каждого вируса специалисты выявляли уникальную последовательность байтов — его сигнатуру. Наличие такой сигнатуры служило высоконадежным индикатором присутствия нежелательного кода, что и заставило авторов вирусов попытаться скрывать любую последовательность байтов, способную выдать присутствие их творений. Они стали делать это посредствам шифрования вирусов.

Первые полиморфные вирусы Tequila и Maltese Amoeba появились в 1991 году. Все бы ничего, но в 1992 году автор, известный под псевдонимом Dark Avenger, написал своего рода комплект «Сделай сам» для мутационного механизма, который он сделал частью вируса Maltese Amoeba.

До 1992 года вирусописатели старались на самом деле зря. Совершенно ясно, что квалификация профессионалов в сфере антивирусной безопасности никак не ниже их собственной и, следовательно, все их многомесячные усилия стоили в крайнем случае лишних часов работы для специалистов. Ведь все зашифрованные вирусы обязательно содержали некий незашифрованный фрагмент: сам расшифровщик или некоторую его часть, по которым можно было построить сигнатуру данного вируса и затем уже бороться с ним обычными способами.

Ситуация изменилась, когда были придуманы алгоритмы, позволяющие не только шифровать код вируса, но и менять расшифровщики. Сама постановка такой задачи

вопросов не вызывает: ясно, что можно построить различные расшифровщики. Суть в том, что этот процесс автоматизирован, и каждая новая копия вируса содержит новый расшифровщик, каждый бит которого может отличаться от битов расшифровщика породившей ее копии.

Некоторые вирусы (например, вирусы семейства Eddie, Murphy) используют часть функций полноценного вируса-невидимки. Обычно они перехватывают функции DOS FindFirst и FindNext и «уменьшают» размер зараженных файлов. Такой вирус невозможно определить по изменению размеров файлов, если, конечно, он резидентно находится в памяти. Программы, которые не используют указанные функции DOS (например, Norton Commander), а напрямую обращаются к содержимому секторов, хранящих каталог, показывают правильную длину зараженных файлов.

При инфицировании файла вирус может производить действия, маскирующие и ускоряющие его распространение.

К подобным действиям можно отнести обработку атрибута Read-only, снятие его перед заражением и последующее восстановление этого атрибута. Многие файловые вирусы считывают дату последней модификации файла и восстанавливают ее после заражения. Для маскировки своего распространения некоторые вирусы перехватывают прерывание DOS, возникающее при обращении к диску, защищенному от записи, и самостоятельно обрабатывают его. Поэтому среди особенностей алгоритма файлового вируса можно назвать наличие или отсутствие обработки и скорость его распространения. Скорость распространения файловых вирусов, заражающих файлы только при их запуске на выполнение, будет ниже, чем у вирусов, заражающих файлы при их открытии, переименовании, изменении их атрибутов и т. д. Некоторые вирусы при создании своей копии в оперативной памяти компьютера пытаются занять область памяти с самыми старшими адресами, разрушая временную часть командного интерпретатора COMMAND.COM. По окончании работы зараженной программы временная часть интерпретатора восстанавливается, при этом происходит открытие файла COMMAND.COM и его заражение, если вирус поражает файлы при их открытии.

Формально macro-вирусы являются файловыми вирусами, заражающими файлы некоторых систем обработки документов (например, Word for Windows, Excel for Windows и AmiPro). Указанные системы имеют встроенные макро-языки (Word Basic, Visual Basic). Эти языки обладают достаточными возможностями, чтобы производить практически все операции, необходимые вирусу. Имеются даже шифрованные и полиморфные macro-вирусы. Кроме того, все чаще стали встречаться вирусы, поражающие как документы, так и исполняемые файлы (иногда обычные EXE-файлы, иногда NewEXE, иногда и те, и другие). Инфицирующая способность таких вирусов крайне велика.

В настоящий момент более 90% macro-вирусов написаны для Word for Windows. Это без сомнения объясняется тем, что файлы данного текстового процессора фактически стали стандартом для текстовых документов. Самый первый macro-вирус (Word. Concept) также заражал DOC-файлы.

Большинство макро-вирусов имеют типичную структуру. Они начинаются с автоматически выполняющегося макроса, заражающего глобальный шаблон Normal.dot. Также в их состав входят некоторые макросы, которые заражают файлы при определенных действиях (File > Save As, File > Save и Tools > Macros). Документы заражаются при совершении над ними операций, то есть инфицируются уже при открытии.

Макрос — это программа, написанная на некотором языке, обычно используемая для автоматизации определенных процессов внутри приложений. В данном случае разговор пойдет о языках Visual Basic for Applications (VBA) и WordBasic (WB), которые применяет Microsoft в своих программах (в частности, Excel, Project и PowerPoint используют язык VBA, а WinWord — WB).

Макрос VBA представляет собой вызываемые процедуры. Они бывают двух типов:

- процедуры-подпрограммы;
- процедуры-функции.

Процедуры-подпрограммы могут выполняться непосредственно или вызываться из других макросов. Конечно, в документ можно вставить столько макросов, сколько нужно (или сколько хочется), ограничений на их количество нет. Набор макросов (процедур-подпрограмм и процедур-функций), входящих в документ, называется модулем VBA.

Язык VBA универсален, и тому есть несколько причин.

1. Этот язык прост в изучении и использовании. Поскольку он является языком визуального программирования, то ориентирован на события, а не на объекты. С его помощью без особых затрат времени очень легко создавать сложные модули.

2. Можно использовать большое количество предопределенных функций, облегчающих работу.

3. Имеются функции (или макросы), выполняющиеся автоматически, за счет чего упрощается написание процедур автокопирования и занесения в память, используемых стандартными DOS-вирусами.

Существуют функции, единые для всех версий языка VBA вне зависимости от используемого языка (английского, русского, испанского и т. д.). Таких специальных макросов 5, все они выполняются автоматически:

- AutoExec — активизируется при загрузке текстового процессора, но только в том случае, если он сохранен в шаблоне Normal.dot или в каталоге стандартных приложений;
- AutoNew — активизируется при создании нового документа;
- AutoOpen — активизируется при открытии существующего документа;
- AutoClose — активизируется при закрытии документа;
- AutoExit — активизируется при выходе из текстового процессора.

Процедура SaveAs использует технологию, во многом схожую с процедурой AutoExec. Она копирует макро-вирус в активный документ при его сохранении через команду File > SaveAs.

Существует несколько способов скрыть вирус или сделать его более эффективным. Например, можно создать специальный макрос, прячущий вирус, если меню Tools > Macro открывается для просмотра.

Макро-вирусы также могут включать внешние процедуры. Например, вирус Nuclear пытается откомпилировать и запустить внешний файл-разносчик вируса, некоторые троянские макросы форматируют винчестер при открытии документа.

Рассмотрим несколько подробнее, как действуют наиболее распространенные вирусы, их особенности, способы внедрения и осуществления разрушительных воздействий.

Начнем с вирусов, поражающих файлы с расширением COM (COM-файлы). Существует несколько способов внедрения таких вирусов.

Структура стандартного COM-файла (программы) предельно проста. Он содержит только код и данные программы, не имея даже заголовка. В начале COM-файла обычно находится команда безусловного перехода JMP, состоящая из трех байт. Благодаря простому строению COM-файла в него очень просто добавить тело вируса и затем указать его адрес в команде JMP.

После старта вирус ищет в текущем каталоге COM-файлы. После нахождения нужного файла тело вируса добавляется в конец этого файла, туда же переносится оригинальный адрес перехода по JMP, на место которого записывается адрес команды JMP для безусловного перехода на тело вируса.

После загрузки зараженного файла управление получает вирус. Закончив работу, он восстанавливает оригинальный адрес безусловного перехода JMP и передает управление программе, как это показано на рис. 2.19.

После того как вирус закончит свою работу, он восстанавливает в исходное состояние первые три байта программы (в памяти компьютера) и передает управление на начало программы. Далее, при запуске зараженного файла, управление сначала получает вирус, и только затем — исходная программа. Благодаря такой схеме работы рассматриваемый вирус может спокойно существовать, будучи «выпущенным на волю» один раз.

Кроме такого способа внедрения, существуют и другие способы внедрения COM-вирусов. Рассмотрим два варианта внедрения COM-вируса в начало файла:

1. Чтобы освободить место для себя, вирус переписывает начало программы в конец файла. После этого тело вируса записывается в начало файла, а небольшая его часть, обеспечивающая перенос вытесненного фрагмента программы, — в конец файла. При восстановлении первоначального вида программы тело вируса будет затерто, поэтому код вируса, восстанавливающий программу, должен находиться в безопасном месте, отдельно от основного тела вируса. Схема этого способа внедрения изображена на рис. 2.20.

При загрузке файла, зараженного таким способом, управление получит вирус (так как он находится в начале файла). По окончании работы вирус передает управление коду, переносящему вытесненную часть программы на прежнее место. После восстановления (в памяти, не в файле) первоначального вида программы, она запускается.

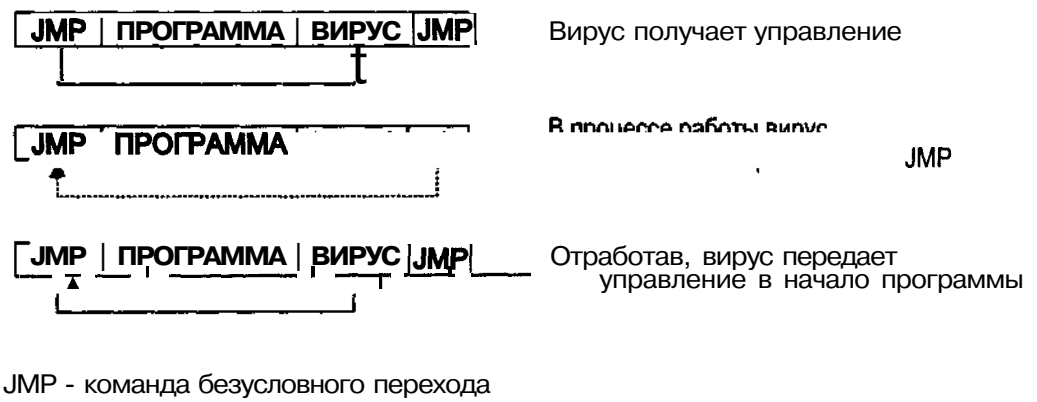


Рис. 2.19. Внедрение comcom-вируса в конец файла и его работа

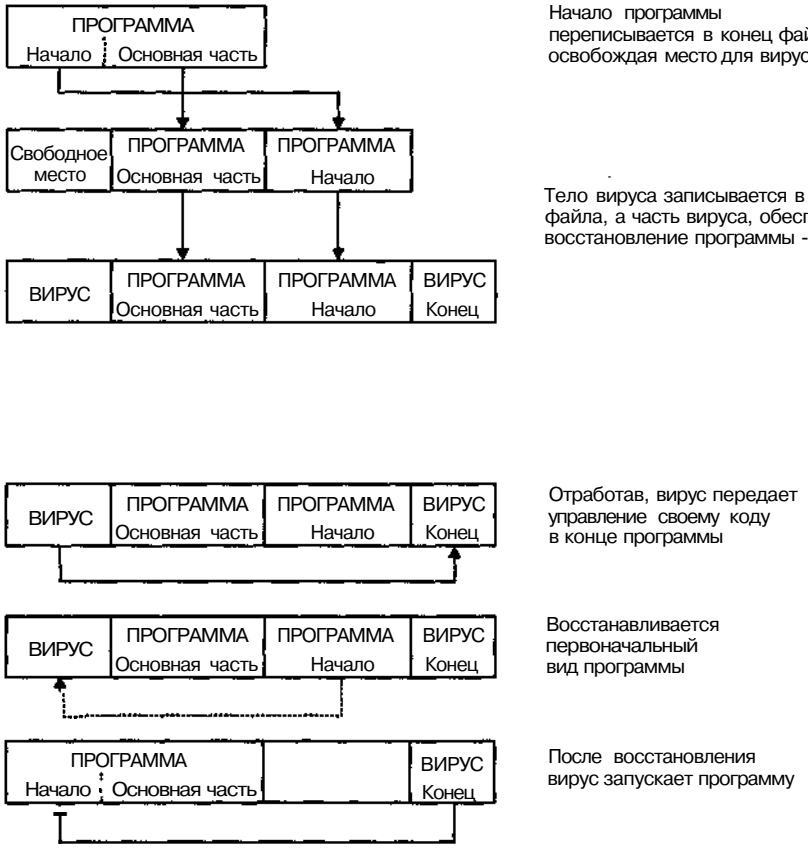


Рис. 2.20. Внедрение и работа corn-вируса, дописывающего свою часть в конец файла

2. Второй вариант отличается от первого тем, что вирус, освобождая для себя место, сдвигает все тело программы, а не переносит ее часть в конец файла. Этот способ внедрения и схема работы вируса изображены на рис. 2.21.

После запуска зараженной программы, как и в предыдущем случае, управление получает вирус. Дальнейшая работа вируса отличается только тем, что часть вируса, восстанавливающая первоначальный вид программы, переносит все тело программы, а не только вытесненную часть

Кроме указанных, существуют вирусы, не дописывающие часть своего тела в конец файла. К примеру, вирус может внедряться в середину файла. В этом случае алгоритм работы вируса является смесью алгоритмов, рассмотренных выше.

COM-файлы (небольшие программы, написанные, в основном, на языке Assembler) со временем устаревают, поэтому им на смену пришли пугающие своими размерами EXE-файлы. Появились и вирусы, умеющие эти файлы заражать.

По особенностям алгоритма, EXE-вирусы условно можно разделить на следующие группы:

- вирусы, замещающие программный код (Overwrite);
- вирусы-спутники (Companion);
- вирусы, внедряющиеся в программу (Parasitic).

Вирусы, замещающие программный код, уже стали раритетом: фактически вирусы данного вида давно мертвы. Изредка появляются еще такие вирусы, созданные на языке Assembler, но это, скорее, соревнование в написании самого маленького overwrite-вируса. Главный их недостаток — слишком грубая работа. Инфицированные ими программы не исполняются, так как вирус записывается поверх программного кода, не сохраняя его. При запуске вирус ищет очередную жертву (или жертвы), открывает найденный файл для редактирования и записывает свое тело в начало программы, не сохраняя оригинальный код. Инфицированные этими вирусами программы лечению не подлежат.

Вирусы-спутники получили такое название из-за алгоритма их размножения: для каждого инфицированного файла создается файл-спутник. Рассмотрим более подробно два типа вирусов этой группы, отличающихся методом заражения файлов:

- путем создания COM-файла спутника;
- путем переименования EXE-файла.

Инфицирование методом создания COM-файла спутника заключается в том, чтобы, не трогая файл (EXE-программу), создать свою — COM-файл с именем EXE-про-

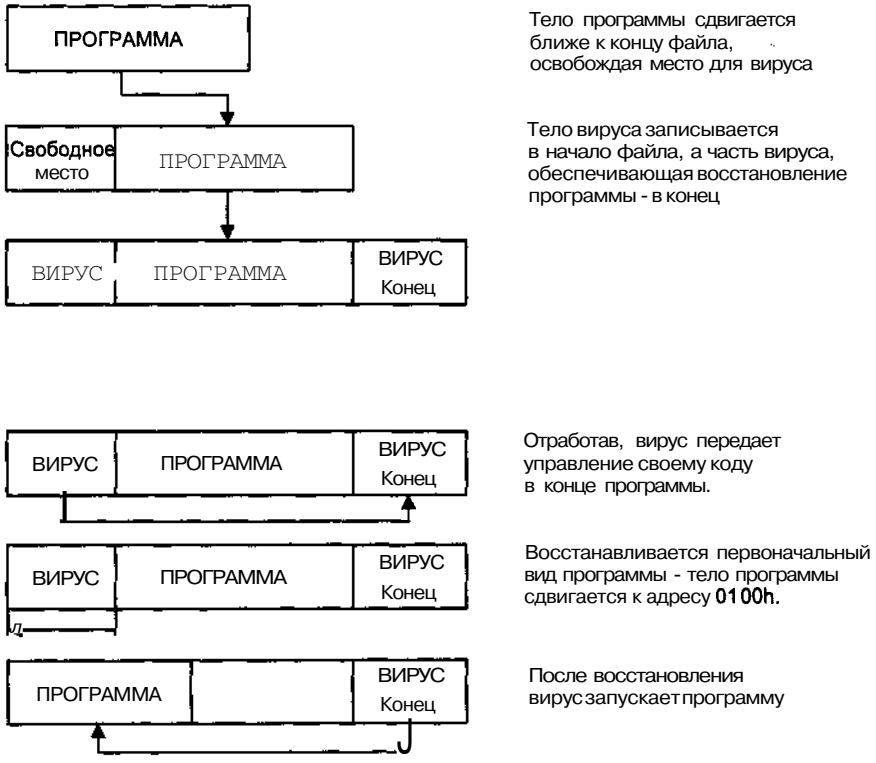


Рис. 2.21. Внедрение и работа corn-вируса, сдвигающего программу

граммы. Алгоритм работы такого вируса предельно прост, так как не нужны лишние действия: например, сохранение в теле вируса размера откомпилированного EXE-файла с вирусным кодом, считывание в буфер тела вируса, запуск файла, из которого вирус получил управление. Незачем даже хранить метку для определения инфицирования файла.

Для каждого инфицируемого EXE-файла в том же каталоге создается файл с вирусным кодом, имеющий такое же имя, что и EXE-файл, но с расширением COM. Вирус активируется, если при запуске программы в командной строке указано только имя исполняемого файла, без расширения. Дело в том, что DOS сначала ищет в текущем каталоге файл СОФАЙЛ с заданным именем. Если COM-файл с таким именем не найден, отыскивается одноименный EXE-файл. Если и он не найден, DOS попробует обнаружить файл с расширением BAT (командный). В случае отсутствия в текущем каталоге исполняемого файла с указанным именем поиск ведется во всех каталогах. Другими словами, когда пользователь хочет запустить программу и набирает в командной строке только ее имя (обычно так все и делают), первым управление получает вирус, код которого находится в COM-файле. Он создает COM-файл еще к одному или нескольким EXE-файлам (распространяется), а затем исполняет EXE-файл с именем, указанным в командной строке. Пользователь же думает, что работает только запущенная EXE-программа. Вирус-спутник обезвредить довольно просто — достаточно удалить COM-файл.

Инфицирование методом переименования EXE-файла несколько совершеннее предыдущего, т. к. для излечения от такого вируса нужно не просто удалить COM-файл с кодом вируса, а разыскать имя переименованного EXE-файла, содержащего инфицированную программу. Что же происходит?

Имя инфицируемого EXE-файла остается прежним, а расширение заменяется каким-либо другим, отличным от исполняемого (COM, EXE, BAT, DAT, OVL и др.). Затем на место EXE-файла копируется вирусный код. При запуске такой инфицированной программы управление получает вирусный код, находящийся в EXE-файле. Инфицировав еще один или несколько EXE-файлов таким же образом, вирус возвращает оригинальному файлу исполняемое расширение (но не EXE, а COM, поскольку EXE-файл с таким именем занят вирусом), после чего исполняет его. Когда работа инфицированной программы закончена, ее запускаемому файлу возвращается расширение неисполняемого. Лечение файлов, зараженных вирусом этого типа, может быть затруднено, если вирус-спутник шифрует часть или все тело инфицируемого файла, а непосредственно перед исполнением его расшифровывает.

Вирусы, внедряющиеся в программу (Parasitic), — самые незаметные. Их код записывается в программы, что существенно затрудняет лечение зараженных файлов и дает этому вирусу много преимуществ перед всеми вышеописанными вирусами: на диске не появляются лишние файлы, нет забот с копированием и переименованием файлов. Рассмотрим методы внедрения EXE-вирусов в EXE-файл. Эти вирусы условно можно разделить на три категории, использующие:

- стандартное заражение EXE -файлов;
- сдвиг;
- перенос.

При стандартном заражении вирус внедряется в конец файла, изменяет заголовок так, чтобы после загрузки файла управление получил вирус. Действие такого вируса мало чем отличается от действия COM-вируса. Оно похоже на заражение COM-файлов, но вместо задания в коде перехода в начало вируса корректируется собственно адрес точки запуска программы. После окончания работы вирус берет из сохраненного заголовка оригинальный адрес запуска программы, прибавляет к его сегментному компоненту значение регистра DS или ES (полученное при старте вируса) и передает управление на полученный адрес.

Внедрение вируса способом сдвига основано на размещении вируса в начале файла со сдвигом кода программы. Механизм заражения такой: тело инфицируемой программы считывается в память, на ее место записывается код вируса, а на место последнего — код инфицируемой программы. Таким образом, код программы как бы «сдвигается» в файле на длину кода вируса. Отсюда и название способа — «способ сдвига». При запуске инфицированного файла вирус заражает еще один или несколько файлов. После этого он считывает в память код программы, записывает его в специально созданный на диске временный файл с расширением исполняемого файла (COM или EXE), и затем исполняет этот файл. Когда программа заканчивает работу, временный файл удаляется. Если при создании вируса не применялось дополнительных приемов защиты, то вылечить инфицированный файл очень просто. Для этого достаточно удалить код вируса в начале файла и программа снова будет работоспособной. Недостаток этого метода заключается в том, что нужно считывать в память весь код инфицируемой программы.

Способ заражения файлов методом переноса — самый совершенный из всех перечисленных. Вирусы, использующие для внедрения перенос, размножаются следующим образом. Из инфицируемой программы от начала файла считывается часть кода, по размеру равная длине вируса. На освободившееся место вписывается вирус, а оригинальное начало программы переносится в конец файла. Отсюда и название метода. После того как вирус инфицировал один или несколько файлов, он выполняет программу, из которой запустился. Для этого он считывает начало инфицированной программы, сохраненное в конце файла, и записывает его в начало файла, восстанавливая работоспособность программы. Затем вирус удаляет код начала программы из конца файла, восстанавливая оригинальную длину файла, и исполняет программу. После завершения программы вирус вновь записывает свой код в начало файла, а оригинальное начало программы — в конец. Этим методом могут быть инфицированы даже антивирусы, которые проверяют свой код на целостность, так как запускаемая вирусом программа имеет точно такой же код, как и до заражения.

Есть и другие варианты. Иногда, например, начало программы записывается в середину файла, а середина переносится в конец, чтобы еще сильнее все запутать. Преимущество данного метода над другими состоит в том, что инфицированная программа исполняется в том же виде, в каком она была до заражения: из файла с тем же именем и расширением, то есть программы, проверяющие себя на предмет заражения, не замечают вируса.

Недостаток данного метода проявляется при сбоях в работе компьютера. Если при исполнении инфицированной программы компьютер зависнет или произойдет перезагрузка системы, инфицированная программа окажется «чистой», без вируса.

Шпионские программные закладки

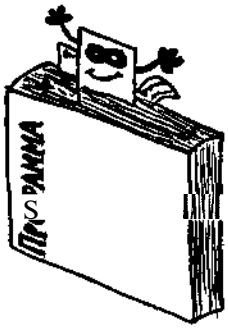
Главным условием правильного функционирования любой компьютерной системы является обеспечение защиты от вмешательства в процесс обработки информации тех программ, присутствие которых в компьютерной системе не обязательно.

По мере развития средств защиты компьютерных систем совершенствуются и средства нападения на них. Одной из самых больших угроз для этих систем является атака посредством использования программных закладок.

Программная закладка — это программа, скрытно внедренная в защищенную систему (или дописанный фрагмент пользовательской программы), позволяющая злоумышленнику путем модификации свойств системы защиты осуществлять несанкционированный доступ к ресурсам системы (в частности, к конфиденциальной информации). Если программная закладка написана грамотно, то после внедрения в систему обнаружить ее стандартными средствами администрирования практически невозможно, она может функционировать неограниченно долгое время, и злоумышленник, внедривший закладку, имеет практически неограниченный доступ к системным ресурсам. Деструктивные действия, осуществляемые программными закладками, представлены на рис. 2.22.

Опасность программных закладок заключается в том, что они, являясь частью защищенной системы, способны принимать активные меры для маскировки своего присутствия в системе. При внедрении закладки в защищенной системе создается скрытый канал информационного обмена, который, как правило, остается незамеченным администратором системы в течение длительного времени. Практически все известные программные закладки, применявшиеся в разное время различными злоумышленниками, были выявлены либо из-за ошибок, допущенных при программировании закладки, либо чисто случайно.

Перспективным направлением является внедрение программных закладок. Их задачей может быть получение информации о паролях, кодовых комбинациях, обрабатываемых данных, а также передача собранных сведений по заданному адресу в сети или по электронной почте. Эта угроза быстро может стать реальностью благодаря возможности «доставки» подобных программ в требуемый компьютер. Собственно, способы те же, что и для компьютерных вирусов, да и сами закладки, по существу, являются вирусами. Классификация программных закладок в соответствии с методами их внедрения в компьютерную сеть представлена на рис. 2.23.



Известны основные механизмы проникновения закладок:

О непосредственное подключение;

G косвенное подключение.

Непосредственное подключение — передача вирусов через средства обмена, используемые в атакуемой системе. Внедрение закладок производится через наименее защищенные узлы системы либо установкой зараженного программного обеспечения.

Косвенное подключение — это проникновение в систему через подсистемы, не служащие ее основному предназначению (электропитание, стабилизация и т. д.). Один из приемов — вне-

дрение вирусов путем подачи электромагнитных импульсов в схему питания. Над этим работают японцы и американцы.

Эксперты отмечают, что программные закладки можно достаточно эффективно применять в военных целях как активный элемент информационно-кибернетического противодействия. При этом они подчеркивают, что чем выше степень компьютеризации систем военного назначения, тем больше вероятность появления закладок. По мнению западных специалистов, программная закладка может быть реализована в виде нескольких команд и иметь сложный механизм активизации, настроенный на условия реального боевого применения системы информационного оружия либо на строго определенную комбинацию входных данных. Закладка может быть включена в состав как общего программного обеспечения вычислительной установки, так и специальных (прикладных) программных средств.

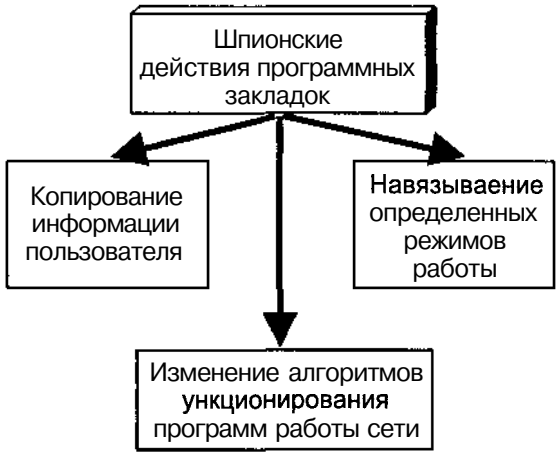


Рис. 2.22. Деструктивные действия, осуществляемые программными закладками

Программные закладки разделяются на автоматические и управляемые. Первые, как правило, заранее настроены (прямо или косвенно) на условия реального боевого применения систем информационного оружия либо боевого управления, а вторые активизируются извне (например, посредством «электронной закладки»). Обнаружить программную закладку сложно, так как она может быть замаскирована.

В иностранной прессе в качестве иллюстрации такой ситуации приводится военный конфликт в Персидском заливе. Система ПВО Ирака оказалась заблокированной по неизвестной причине во время проведения операции «Буря в пустыне». В результате иракская сторона была вынуждена оставить без ответа бомбовые удары по своей территории. Несмотря на отсутствие исчерпывающей информации, многие иностранные специалисты высказывают предположение, что закупленные Ираком у Франции ЭВМ, входящие в комплекс технических средств системы ПВО, содержали специальные управляемые электронные закладки, блокировавшие работу вычислительной системы. Если они правильно оценивают события, это означает, что начался такой этап, когда при ведении боевых действий появилась возможность применять новое электронно-информационное оружие.

Шпионские программные закладки могут выполнять хотя бы одно из перечисленных ниже действий:

- вносить произвольные искажения в коды программ, находящихся в оперативной памяти компьютера (программная закладка первого типа);
- переносить данные из одних областей оперативной или внешней памяти компьютера в другие (программная закладка второго типа);

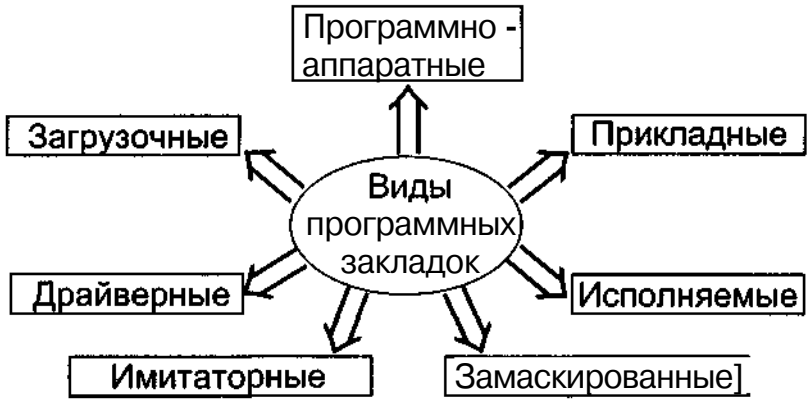


Рис. 2.23. Виды программныех закладки, классифицированныеок по методу их внедрения в сеть

- искажать информацию, выводимую на внешние устройства или в канал связи, полученную в результате работы других программ (программная закладка третьего типа).

Программные закладки можно классифицировать и по методу их внедрения в компьютерную систему:

- программно-аппаратные закладки, ассоциированные с аппаратными средствами компьютера (их средой обитания, как правило, является BIOS — набор программ, записанных в виде машинного кода в ПЗУ);
- загрузочные закладки, связанные с программами начальной загрузки, которые располагаются в загрузочных секторах (из этих секторов в процессе выполнения начальной загрузки компьютер считывает программу, берущую на себя управление для последующей загрузки самой операционной системы);
- драйверные закладки, ассоциированные с драйверами (файлами, в которых содержится информация, необходимая операционной системе для управления подключенными к компьютеру периферийными устройствами);
- прикладные закладки в прикладном программном обеспечении общего назначения (текстовые редакторы, утилиты, антивирусные мониторы и программные оболочки);
- исполняемые закладки в исполняемых программных модулях, содержащих ее код (чаще всего эти модули представляют собой пакетные файлы, т. е. файлы, которые состоят из команд операционной системы, выполняемых одна за одной, как если бы их набирали на клавиатуре компьютера);
- закладки-имитаторы, интерфейс которых совпадает с интерфейсом некоторых служебных программ, требующих ввести конфиденциальную информацию (пароль, криптографический ключ, номер кредитной карточки);
- замаскированные закладки, которые маскируются под программные средства оптимизации работы компьютера (файловые архиваторы, дисковые дефрагментаторы) или под программы игрового и развлекательного назначения.

Все программные закладки (независимо от их назначения, метода внедрения в компьютерную систему, а также срока пребывания в оперативной памяти) имеют одну важную особенность: они обязательно выполняют операцию записи в оперативную или внешнюю память системы. Если бы они не делали этого, то не могли бы оказать никакого негативного влияния. Ясно, что для целенаправленного воздействия закладка должна выполнять и операцию чтения, иначе в ней может быть реализована только функция разрушения (например, удаление или замена информации в определенных секторах жесткого диска).

С учетом замечания о том, что программная закладка должна быть обязательно загружена в оперативную память компьютера, можно подразделить закладки на:

- резидентные;
- нерезидентные.

Резидентные закладки находятся в оперативной памяти постоянно, начиная с некоторого момента и до окончания сеанса работы компьютера, т. е. до его перезагрузки или до выключения питания.

Нерезидентные закладки попадают в оперативную память компьютера аналогично резидентным, однако, в отличие от резидентных, выгружаются по истечении некоторого времени или при выполнении каких-либо условий.

Иногда сам пользователь провоцирует запуск исполняемого файла, содержащего код программной закладки. Известен такой случай. Среди пользователей свободно распространялся набор из архивированных файлов. Для извлечения файлов из него требовалось вызвать специальную утилиту, которая запускается после указания ее имени в командной строке. Однако мало кто из пользователей замечал, что в полученном наборе файлов уже имелась программа с таким же именем и что запускалась именно она. Кроме разархивирования файлов, эта программная закладка дополнительно производила действия негативного характера.

Среди программистов популярны пословицы: «Каждая последняя ошибка в программе на самом деле является предпоследней» и «Если программа работает без ошибок, это — Hello world (простейшая программа, с которой начинается большинство учебников программирования)». Предполагать, что программное обеспечение системы защиты не содержит ошибок, наивно: ошибки, позволяющие злоумышленникам осуществлять НСД к ресурсам системы, время от времени обнаруживаются практически во всех системах защиты. И если такая ошибка в системе присутствует, злоумышленник может использовать ее для внедрения программной закладки. Известно множество примеров использования злоумышленниками подобных ошибок, в том числе и для внедрения программных закладок.

Даже если программное обеспечение системы защиты не содержит ошибок (что маловероятно), имеется реальная возможность внедрения программной закладки из-за неправильного проведения политики безопасности.

На самом деле указанный в сертификате класс защиты говорит всего лишь о верхнем уровне защищенности программ и данных. Даже если система защиты сертифицирована по некоторому классу, это вовсе не означает, что она надежно защищена от программных закладок. Практически все конфигурации защищенных компьютерных систем, реально используемые на практике, уязвимы для программных закладок.

Среди не очень опытных сетевых администраторов распространено мнение, что программные закладки опасны только для тех систем, в которых либо программное обеспечение содержит грубые ошибки, либо администраторы не способны поддерживать необходимую политику безопасности, которая включает в себя реализацию надежной защиты системы от НСД, в том числе к тем ее элементам, доступ к которым необходим для внедрения программной закладки. При этом считается, что если в организации используются только сертифицированные средства защиты и ее администраторы обладают высокой квалификацией, для сети этой организации программные закладки не представляют угрозы. Другими словами, если защитой информации занимаются умные люди, то закладок бояться нечего.

Но даже высококвалифицированные администраторы системы, как и все люди, иногда совершают ошибки, и хотя ошибки достаточно быстро обнаруживаются и устраняются, для того чтобы программная закладка внедрилась в систему, бывает достаточно и 5—10 мин.

Чтобы программная закладка могла что-нибудь сделать с другими программами или с данными, процессор должен приступить к исполнению команд, входящих в состав кода программной закладки. Это возможно только при одновременном соблюдении следующих условий:

- программная закладка должна попасть в оперативную память компьютера (если закладка относится к первому типу, то она должна быть загружена до начала работы программы, являющейся целью воздействия закладки, или во время работы этой программы);
- работа закладки, находящейся в оперативной памяти, начинается при выполнении активизирующих условий.

Существуют три основные группы деструктивных воздействий программных закладок:

- копирование информации (паролей, криптографических ключей, кодов доступа, конфиденциальных электронных документов), находящейся в оперативной или внешней памяти данной системы либо в памяти другой компьютерной системы, подключенной к ней через локальную или глобальную компьютерную сеть;
- изменение алгоритмов функционирования системных, прикладных и служебных программ (например, внесение изменений в программу разграничения доступа может привести к тому, что она разрешит вход в систему всем без исключения пользователям вне зависимости от правильности введенного пароля);
- навязывание определенных режимов работы (например, блокирование записи на диск при удалении информации, при этом информация, которую требуется удалить, не уничтожается и может быть впоследствии скопирована хакером).

Можно выделить следующие характерные модели воздействия программных закладок на компьютерную сеть:

- перехват (перехватчики паролей, клавиатурные шпионы и т. д.);
- искажение;
- уборка мусора;
- наблюдение и компрометация.

Обобщенная модель воздействия программных закладок на компьютерную сеть представлена на рис. 2.24.

В модели «перехват» программная закладка внедряется в ПЗУ, системное или прикладное программное обеспечение и сохраняет всю или выбранную информацию, вводимую с внешних устройств компьютерной системы или выводимую на эти устройства, в скрытой области памяти локальной или удаленной компьютерной системы. Объектом сохранения, например, могут служить символы, введенные с клавиатуры (все повторяемые два раза последовательности символов), или документы, распечатываемые на принтере.

Данная модель может быть двухступенчатой. На первом этапе сохраняются только имена или начала файлов. На втором этапе злоумышленник анализирует накопленные данные и выбирает конкретные объекты для следующей атаки.

В этой модели используются наиболее распространенные программные закладки, перехватывающие пароли пользователей операционных систем — перехватчики паролей. Перехватчики паролей были разработаны для операционных систем OS/370, MS DOS, Windows и UNIX. Внедренный в систему перехватчик паролей получает доступ к паролям, вводимым пользователями при входе в систему. Перехватив очередной пароль, закладка записывает его в специальный файл или в любое другое место, доступное злоумышленнику, внедрившему закладку. Все перехватчики паролей можно подразделить на три основных вида.

Перехватчики паролей первого вида действуют по следующему алгоритму. Злоумышленник запускает программу, которая имитирует приглашение для входа в систему, и ждет ввода. Когда пользователь вводит имя и пароль, закладка сохраняет их в доступном злоумышленнику месте, после чего ее работа завершается и злоумышленник выходит из системы (из большинства операционных систем можно выйти программным путем). По окончании работы закладки на экране появляется настоящее приглашение для входа пользователя в систему.

Пользователь, ставший жертвой закладки, видит, что он не вошел в систему, и что ему снова предлагается ввести имя и пароль. Пользователь предполагает, что при вводе пароля произошла ошибка, и вводит имя и пароль повторно. Он входит в систему и работает нормально. Некоторые закладки, функционирующие по данной схеме, перед завершением работы выдают на экран правдоподобное сообщение об ошибке, например: «Пароль введен неправильно. Попробуйте еще раз».

Основным достоинством этого класса перехватчиков паролей является то, что написание подобной программной закладки не требует от злоумышленника никакой специальной квалификации. Любой пользователь, умеющий программировать хотя бы на языке BASIC, может написать такую программу за считанные часы. Единственная проблема, которая может здесь возникнуть, заключается в программной реализации выхода пользователя из системы. Однако соответству-

Рис 2.24 Модель воздействия программных закладок на компьютерную сеть

ющий системный вызов документирован для всех многопользовательских операционных систем. Если злоумышленник не поленится внимательно изучить документацию по операционной системе, то он решит данную проблему очень быстро.

Перехватчики паролей второго рода перехватывают все данные, вводимые с клавиатуры. Простейшие программные закладки этого типа просто сбрасывают данные на жесткий диск или в любое другое место, доступное злоумышленнику.

Такие программы еще называются клавиатурными шпионами. В специальном текстовом файле они запоминают, какие клавиши были нажаты в ваше отсутствие. Текст, набранный на компьютере, в каком-нибудь бизнес-центре или Internet-кафе, может без особых проблем стать достоянием владельца такого компьютера. Подобные программы разработаны для разных операционных систем, они могут автоматически загружаться при включении компьютера и маскируются под резидентные антивирусы или еще что-нибудь полезное.

Более совершенные закладки анализируют перехваченные данные и отсеивают информацию, заведомо не имеющую отношения к паролям. Несколько таких закладок было написано в разное время для операционной системы MS DOS.

Эти закладки представляют собой резидентные программы, перехватывающие одно или несколько прерываний процессора, имеющих отношение к работе с клавиатурой. Информация о нажатой клавише и введенном символе, возвращаемая этими прерываниями, используется закладками для своих целей.

Любой русификатор клавиатуры, работающий в среде Windows, перехватывает всю информацию, вводимую пользователем с клавиатуры, в том числе и пароли. Несложно написать русификатор так, чтобы он, помимо своих основных функций, выполнял бы и функции перехватчика паролей. Написать программу локализации клавиатуры достаточно просто. Можно встроить перехватчик паролей в цепочку фильтров перед русификатором или после него, так что вся информация, вводимая с клавиатуры, проходит и через русификатор, и через перехватчик паролей. В этом случае задача написания программной закладки, перехватывающей пароли пользователей Windows, становится настолько простой, что не требуется специальная квалификация.

Если операционная система допускает переключение раскладки клавиатуры при вводе пароля, то для этой операционной системы можно написать перехватчик паролей второго рода.

К перехватчикам паролей третьего рода относятся программные закладки, полностью или частично подменяющие собой подсистему аутентификации операционной системы. Поскольку задача создания такой программной закладки гораздо сложнее, чем создание перехватчика паролей первого или второго рода, этот класс программных закладок появился совсем недавно.

Перехватчик паролей третьего рода может быть написан для любой многопользовательской операционной системы. Сложность создания такого перехватчика паролей зависит от сложности алгоритмов, реализуемых подсистемой аутентификации, сложности интерфейса между ее отдельными модулями, а также от степени документированности подсистемы аутентификации операционной системы.

В модели «искажение» программная закладка изменяет информацию, которая записывается в память компьютерной системы в результате работы программ, либо по-

давляет/инициирует возникновение ошибочных ситуаций в компьютерной системе. Можно выделить два типа искажений, использующих данную модель:

- статическое;
- динамическое.

Статическое искажение происходит всего один раз. При этом модифицируются параметры программной среды компьютерной системы, чтобы впоследствии в ней выполнялись нужные злоумышленнику действия. К статическому искажению относится, например, внесение изменений в файл AUTOEXEC.BAT операционной системы Windows 95/98, которые приводят к запуску заданной программы, прежде чем будут запущены все другие, перечисленные в этом файле.

Специалистам российского Федерального агентства правительственной связи и информации (ФАПСИ), например, удалось выявить при анализе одной из отечественных систем цифровой подписи интересное статистическое искажение. Злоумышленник (сотрудник отдела информации финансовой организации, в которой была внедрена данная система) исправил в EXE-модуле программы проверки правильности цифровой подписи символьную строку «ПОДПИСЬ НЕКОРРЕКТНА» на символьную строку «ПОДПИСЬ КОРРЕКТНА». В результате вообще перестали фиксироваться документы с неверными цифровыми подписями, и, следовательно, в электронные документы стало можно вносить произвольные изменения уже после их подписания электронной цифровой подписью.

Динамическое искажение заключается в изменении каких-либо параметров системных или прикладных процессов при помощи заранее активизированных закладок. Динамическое искажение можно условно разделить так:

- искажение на входе (когда на обработку попадает уже искаженный документ);
- искажение на выходе (когда искажается информация, отображаемая для восприятия человеком или предназначенная для работы других программ).

Практика применения цифровой подписи в системах автоматизированного документооборота показала, что именно программная реализация цифровой подписи особенно подвержена влиянию программных закладок типа «динамическое искажение», которые позволяют проводить фальшивые финансовые документы и вмешиваться в процесс разрешения споров по фактам неправомерного применения цифровой подписи. Например, в одной из программных реализаций широко известной криптосистемы PGP электронный документ, под которым требовалось поставить цифровую подпись, считывался блоками по 512 байт, причем процесс считывания считался завершенным, если в блоке данные занимали меньше 512 байт. Работа одной программной закладки, выявленной специалистами ФАПСИ, основывалась на навязывании длины файла. Эта закладка позволяла считывать только первые 512 байт документа, и в результате цифровая подпись определялась на основе этих 512 байт. Такая же схема действовала и при проверке поставленной под документом цифровой подписи. Следовательно, оставшаяся часть этого документа могла быть произвольным образом искажена, и цифровая подпись под ним продолжала оставаться «корректной».

Существуют следующие основные способы воздействия программных закладок на цифровую подпись:

- искажение входной информации (изменяется поступающий на подпись электронный документ);

- искажение результата проверки истинности цифровой подписи (вне зависимости от результатов работы программы цифровая подпись объявляется подлинной);
- навязывание длины электронного документа (программе цифровой подписи предъявляется документ меньшей длины, чем на самом деле, и в результате цифровая подпись ставится только под частью исходного документа);
- искажение программы цифровой подписи (вносятся изменения в исполняемый код программы с целью модификации алгоритма).

В рамках модели «искажение» также реализуются программные закладки, действие которых основывается на инициировании или подавлении сигнала о возникновении ошибочных ситуаций в компьютерной системе, т. е. тех, которые приводят к отличному от нормального завершению исполняемой программы (предписанного соответствующей документацией).

Для инициирования статической ошибки на устройствах хранения информации создается область, при обращении к которой (чтение, запись, форматирование и т. п.) возникает ошибка, что может затруднить или блокировать некоторые нежелательные для злоумышленника действия системных или прикладных программ (например, не позволять корректно уничтожить конфиденциальную информацию на жестком диске).

При инициировании динамической ошибки для некоторой операции генерируется ложная ошибка из числа тех ошибок, которые могут возникать при выполнении данной операции. Например, для блокирования приема или передачи информации в компьютерной системе может постоянно инициироваться ошибочная ситуация «МОДЕМ ЗАНЯТ». Или при прочтении первого блока информации длиной 512 байт может устанавливаться соответствующий флажок для того, чтобы не допустить прочтения второго и последующих блоков и в итоге подделать цифровую подпись.

Чтобы маскировать ошибочные ситуации, злоумышленники обычно используют подавление статической или динамической ошибки. Целью такого подавления часто является стремление блокировать нормальное функционирование компьютерной системы или желание заставить ее неправильно работать. Чрезвычайно важно, чтобы компьютерная система адекватно реагировала на возникновение всех без исключения ошибочных ситуаций, поскольку отсутствие должной реакции на любую ошибку эквивалентно ее подавлению и может быть использовано злоумышленником.

Известен случай успешной атаки пары аргентинских самолетов-торпедоносцев на английский эсминец «Шеффилд», закончившейся нанесением серьезных повреждений этому кораблю. Из-за ошибок в программном обеспечении установленная на нем система противовоздушной обороны не смогла выбрать цель, которую полагалось сбивать первой, поскольку атакующие самолеты летели слишком близко друг от друга.

Разновидностью искажения является также модель типа «троянский конь». В этом случае программная закладка встраивается в постоянно используемое программное обеспечение и по некоторому активизирующему событию вызывает возникновение сбойной ситуации в компьютерной системе. Тем самым достигаются сразу две цели: парализуется ее нормальное функционирование, а злоумышленник, получив доступ к компьютерной системе для устранения неполадок, сможет, например, извлечь из нее информацию, перехваченную другими программными закладками. В качестве активизирующего события обычно используется наступление определенного момента вре-

мени, сигнал из канала модемной связи или состояние некоторых счетчиков (например, счетчика количества запусков программы).

Следующая модель программных закладок называется «уборка мусора». Интересно, почему? Как известно, для хранения данных на внешних носителях прямого доступа выделяется несколько уровней иерархии: сектора, кластеры и файлы. Сектора являются единицами хранения информации на аппаратном уровне. Кластеры состоят из одного или нескольких подряд идущих секторов. Файл — это множество кластеров, связанных по определенному закону.

Работа с конфиденциальными электронными документами обычно сводится к последовательности следующих манипуляций с файлами:

- создание;
- хранение;
- коррекция;
- уничтожение.

Для защиты конфиденциальной информации обычно используется шифрование. Основная угроза исходит отнюдь не от использования нестойких алгоритмов шифрования и «плохих» криптографических ключей (как это может показаться на первый взгляд), а от обыкновенных текстовых редакторов и баз данных, применяемых для создания и коррекции конфиденциальных документов.

Дело в том, что подобные программные средства, как правило, в процессе функционирования создают в оперативной или внешней памяти компьютерной системы временные копии документов, с которыми они работают. Естественно, все эти временные файлы выпадают из поля зрения любых программ шифрования и могут быть использованы злоумышленником для того, чтобы составить представление о содержании хранимых в зашифрованном виде конфиденциальных документов.

Важно помнить и о том, что при записи отредактированной информации меньшего объема в тот же файл, где хранилась исходная информация до начала сеанса ее редактирования, образуются так называемые «хвостовые» кластеры, в которых эта исходная информация полностью сохраняется. И тогда «хвостовые» кластеры не только не подвергаются воздействию программ шифрования, но и остаются незатронутыми даже средствами гарантированного удаления информации. Конечно, рано или поздно информация из «хвостовых» кластеров затирается данными из других файлов, однако по оценкам специалистов ФАПСИ из «хвостовых» кластеров через сутки можно извлечь до 85%, а через десять суток — до 25—40% исходной информации.

Пользователям необходимо иметь в виду и то, что команда удаления файла (DEL) операционной системы DOS не изменяет содержания файла, и оно может быть в любой момент восстановлено, если поверх него еще не был записан другой файл. Распространенные средства гарантированного стирания файлов предварительно записывают на его место константы или случайные числа и только после этого удаляют файл стандартными средствами DOS. Однако даже такие мощные средства оказываются бессильными против программных закладок, которые нацелены на то, чтобы увеличить количество остающихся в виде «мусора» фрагментов конфиденциальной информации. Например, программная закладка может инициировать статическую ошибку, пометив один или несколько кластеров из цепочки, входящей в файл, меткой «СБОЙНЫЙ». В результате при удалении файла средствами операционной системы или сред-

ствами гарантированного уничтожения та его часть, которая размещена в сбойных кластерах, останется нетронутой и впоследствии может быть восстановлена с помощью стандартных утилит.

И, наконец, последняя модель — наблюдение и компрометация. Помимо перечисленных, существуют и другие модели воздействия программных закладок на компьютеры. В частности, при использовании модели типа «наблюдение» программная закладка встраивается в сетевое или телекоммуникационное программное обеспечение. Пользуясь тем, что подобное программное обеспечение всегда находится в активном состоянии, внедренная в него программная закладка может следить за всеми процессами обработки информации в компьютерной системе, а также устанавливать и удалять другие программные закладки.

Модель типа «компрометация» позволяет получать доступ к информации, перехваченной другими программными закладками. Например, инициируется постоянное обращение к такой информации, приводящее к росту соотношения сигнал/шум. А это, в свою очередь, значительно облегчает перехват побочных излучений данной компьютерной системы и позволяет эффективно выделять сигналы, сгенерированные закладкой типа «компрометация», из общего излучения, исходящего от оборудования.

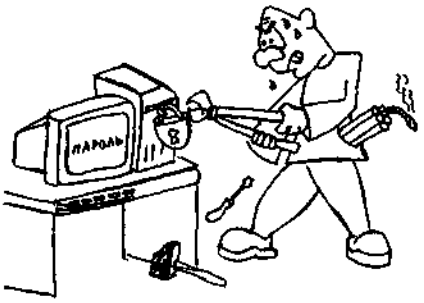
Силовые деструктивные воздействия на информационные системы

Возрастающие технологические возможности обработки информации находят все большее применение в таких жизненно важных сферах, как телекоммуникация, энергетика, системы хранения нефти и газа, финансовая и банковская системы, оборона и национальная безопасность, авиационные диспетчерские системы. Все это и может явиться лакомым куском для современных террористов. В последние годы стала усиленно развиваться одна из ветвей информационного терроризма, о которой еще с десяток лет назад никто и не задумывался, — это так называемый электромагнитный терроризм. Применяя его, террористы могут без лишнего шума воздействовать на технические системы государственного и военного управления и объекты инфраструктуры.

Благодаря активному развитию современных информационных технологий и систем безопасности появилась не только возможность успешно решать задачи обеспечения безопасности личности, объектов и информации, но и возникли новые проблемы. Одна из этих проблем — защита самих систем от силового разрушающего воздействия.

Современные технические средства силового разрушающего или поражающего (деструктивного) воздействия являются по существу электромагнитным оружием, которое способно дистанционно и без лишнего шума поразить практически любую информационную систему.

Главное в этом случае — обеспечить соответствующую мощность электромагнитного импульса, воздействующего на систему по цепям питания или по каналам связи. Иначе говоря, компьютер или любое другое электронное оборудование информацион-



ной системы могут быть подвергнуты, с учетом среды передачи энергии, силовому деструктивному воздействию (рис. 2.25) по трем основным каналам:

- сети питания;
- проводным линиям связи;
- эфиру с использованием мощных коротких электромагнитных импульсов.

Простейшим примером мощного электромагнитного импульса является обычное и привычное для всех нас природное явление — молния. Это естественный электромагнитный импульс, воздействующий на различные радиоэлектронные устройства.

Поскольку мы рассматриваем в основном преднамеренные деструктивные воздействия на элементы компьютерных сетей, то остановимся более подробно на рассмотрении электромагнитных импульсов искусственного происхождения.

Первое преднамеренное воздействие на электронные средства было проведено еще на заре развития радиосвязи, необходимой для управления войсками на больших расстояниях без использования проводов. И началось это электронное противодействие с, казалось бы, незаметного эпизода русско-японской войны. 15 апреля 1904 года с помощью радиостанции броненосца «Потемкин» была сорвана корректировка огня

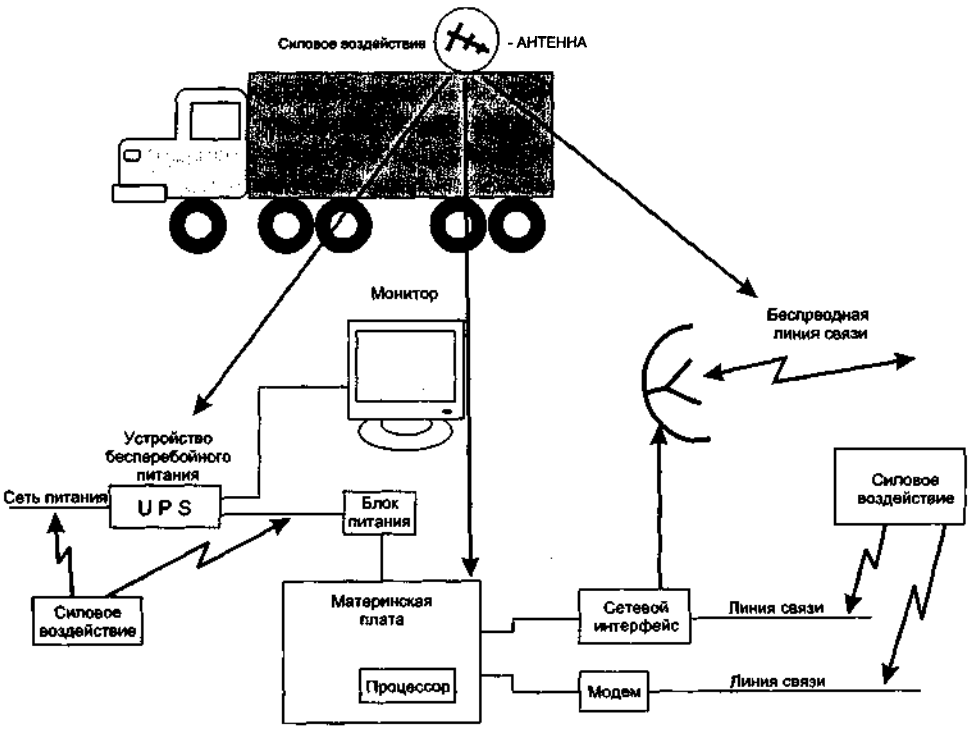


Рис. 2.25. Основные каналы деструктивного воздействия на компьютерные системы

японских крейсеров. Это исторический факт, подтвержденный как российскими, так и японскими архивными документами.

По сегодняшним меркам, такое воздействие можно сравнить с работой сварочного аппарата. Но наука не стояла на месте. И уже в 1945 году физиками-теоретиками было предсказано появление мощного электромагнитного импульса при взрыве ядерного устройства. А в конце 50-х — начале 60-х годов прошлого века, во время проводившихся ядерных взрывов в атмосфере и в космическом пространстве, наличие мощного электромагнитного импульса было зафиксировано экспериментально. Однако изучением этого явления в те годы занимались не достаточно интенсивно, поскольку в радиоэлектронном оборудовании того времени использовались исключительно электровакуумные приборы, которые мало подвержены влиянию электромагнитных импульсов.

Новый толчок к изучению электромагнитных импульсов произошел с появлением полупроводниковой техники. На ее основе развивалась цифровая электронная техника и, следовательно, информационные технологии, проникшие в настоящее время практически во все сферы деятельности человека.

На сегодняшний день уже разработаны специальные виды «электромагнитного оружия», способные генерировать электромагнитные импульсы огромной мощности, значительно превышающей электромагнитные импульсы, возникающие при ядерном взрыве. Такое оружие производится в виде боеголовок для ракет, бомб, специальных «высокочастотных пушек» и т. п. Для генерации поражающих электромагнитных импульсов созданы компактные, мобильные и одновременно мощные устройства.

Электромагнитное оружие некоторых видов было испытано США при проведении военных операций в Ираке и Югославии. В случае внезапного нападения эффективным стратегическим приемом нападающей стороны является достижение у противника «электронного шока» еще до первого выстрела. Во время успешного нападения израильских спецслужб на виллу одного из лидеров палестинского сопротивления Абу-Нидаля средства связи, которыми располагала охрана особняка, были выведены из строя дистанционным воздействием мощного электромагнитного импульса с пролетавшего в отдалении самолета. Похожий прием был использован в шестидневной арабо-израильской войне 1967 года, когда средства радиоэлектронного воздействия были использованы массированно в течение 2 часов (1,5% продолжительности активных боевых действий). В войне в зоне Персидского залива «электронный удар» продолжался одни сутки (~2,5% продолжительности боевых действий).

Для поражения гражданских объектов вполне может быть достаточно воздействия электромагнитных импульсов сравнительно небольшой мощности. Технические средства, с помощью которых они получаются, носят название технических средств силового деструктивного воздействия. В Internet можно встретить подробные руководства по созданию установок для генерации электромагнитных импульсов с целью поражения компьютеров, компьютерных сетей и другого электронного оборудования. Необходимые комплектующие можно купить в обычных магазинах. С помощью таких устройств можно, например, вывести из строя компьютер соседа, находящийся за стеной. Есть устройства, размещающиеся в обычном кейсе, которые способны вывести из строя 10—20 компьютеров среднего банка. Более мощные установки можно поместить в фургоне автомобиля. Стоимость таких устройств, в зависимости от их конструкции, размеров и мощности, составляет от 300 до 20 000 долларов. Такие суммы по карману даже террористу-одиночке.

Последствия же электромагнитного терроризма могут быть самыми чудовищными. Скрытность применения технических средств деструктивного воздействия, компактность, высокая проникающая способность и эффективность действия, делают их идеальными орудиями преступления в руках террористов и других злоумышленников.

Эти средства могут быть использованы, например, для уничтожения компьютерной сети банка, в котором деньги предварительно были похищены хакерами. Они позволяют обеспечить беспрепятственное проникновение на охраняемый объект, преднамеренно разрушив систему охранной сигнализации или блокировав ее работу.

Такого рода «электронный рэкет» для предприятий с большой долей электронного документооборота может оказаться гораздо опаснее, нежели традиционные приемы, применяемые криминальными структурами.

По свидетельству официальных источников (администрация президента США, Агентство национальной безопасности (АНБ) США, Скотланд Ярд и др.), еще в 1997 году отмечены случаи атак с использованием технических средств деструктивного воздействия на жизненно важные электронные системы западных стран. Эти же источники подтвердили, что многие финансовые структуры США тайно платили бандам преступников, чтобы предотвратить разрушение своих компьютерных систем. По мнению АНБ (данные на 1996 год), в мире существовало по крайней мере четыре таких организованных банды.

В отличие от других способов уничтожения информации, оборудования или методов проникновения на охраняемый объект, применение технических средств деструктивного воздействия требует существенно меньших интеллектуальных, а нередко и материальных затрат. Кроме того, последствия от такой атаки на объект могут быть отнесены пострадавшими на обычные нарушения функционирования объекта, например, нарушения в сети электропитания объекта.

Перед тем как рассматривать различные деструктивные воздействия на технические средства информационных комплексов, сделаем обзор нормативных документов, согласно которым производится тестирование электронной техники.

В нашей стране и за рубежом все компьютеры и другая электронная техника проходят тестирование на предмет их правильного функционирования в сложных условиях электромагнитной обстановки. ГОСТ 29073-91 («Совместимость технических средств измерения, контроля и управления промышленными процессами электромагнитная. Устойчивость к электромагнитным помехам. Общие положения».) устанавливает общие требования к техническим средствам в соответствии со стандартом МЭК 801 по устойчивости к воздействию электромагнитных помех (помехоустойчивость) следующих видов:

О электростатических разрядов;

- наносекундных и микросекундных импульсных помех;
- радиочастотных электромагнитных помех;
- динамических изменений напряжения сети электропитания.

Согласно этому документу, технические средства должны сохранять работоспособность в условиях эксплуатации при воздействии электромагнитных помех, создаваемых промышленным оборудованием различного назначения, сетью электропитания, молниями и электростатическими разрядами. Все испытания проводят во время функционирования технических средств, а для качественной оценки используются показатели, представленные в табл. 2.2.

Таблица 2.2. Критерии качества функционирования технических средств

Критерии качества функционирования технических средств при испытаниях на помехоустойчивость	Качество функционирования технических средств при испытаниях на помехоустойчивость
A	Нормальное функционирование в соответствии с техническими условиями
B	Кратковременное нарушение функционирования или ухудшение параметров с последующим восстановлением нормального функционирования без вмешательства оператора
C	Кратковременное нарушение функционирования или ухудшение параметров, требующее для восстановления нормального функционирования вмешательства оператора
D	Нарушение функционирования или ухудшение параметров, требующее ремонта из-за выхода из строя оборудования или компонентов

Другой руководящий документ — ГОСТ 29191-91 (МЭК 801-2 — 88) «Совместимость технических средств электромагнитная. Устойчивость к электростатическим разрядам. Технические требования и методы испытаний» — относится к группе государственных стандартов, регламентирующих устойчивость технических средств к электромагнитным помехам различного вида. Он подразделяет технические средства по степени жесткости испытаний (табл. 2.3) в зависимости от испытательного напряжения.

Таблица 2.3. Значения испытательного напряжения по степени жесткости.

Степень жесткости	Испытательное напряжение, кВ	
	Контактный разряд	Воздушный разряд
1	2	2
2	4	4
3	6	8
4	8	15
5	По согласованию между потребителем и производителем	

Основной целью стандарта ГОСТ 29156-91 (МЭК 801-4-88) «Совместимость технических средств электромагнитная. Устойчивость к наносекундным импульсным помехам. Технические требования и методы испытаний» является установление общих методов оценки качества функционирования технических средств при воздействии наносекундных импульсных помех на цепи силового электропитания и цепи ввода/вывода. Согласно этому документу, для испытаний устанавливаются степени жесткости, которые представлены в табл. 2.4.

Как видно из табл. 2.4, степень жесткости 1 устанавливается для очень хорошей электромагнитной обстановки. Для данной степени жесткости в лабораториях испытания ограничивают воздействием коротких импульсных помех на цепи электропитания, а в условиях эксплуатации — воздействием на цепи заземления проверяемых технических средств.

Таблица 2.4. Степени жесткости по устойчивости технических средств к воздействию импульсных помех

Степень жесткости	Амплитуда импульсов выходного напряжения ненагруженного испытательного генератора	
	Цепь силового электропитания, кВ	Сигнальные цепи ввода/вывода, кВ
1	0,5	0,25
2	1,0	0,5
3	2,0	1,0
4	4,0	2,0
5	По согласованию между потребителем и производителем	

Степень жесткости 2 устанавливается для хорошей электромагнитной обстановки. Примером условий, соответствующих этой степени жесткости, может служить электромагнитная обстановка в помещении для средств измерения, контроля и управления на промышленном или энергетическом предприятии.

Степень жесткости 3 устанавливается для промышленной электромагнитной обстановки. Примером условий, соответствующих степени жесткости 3, может служить электромагнитная обстановка на предприятиях энергетики и в релейных помещениях на подстанциях воздушных линий высокого напряжения.

Степень жесткости 4 устанавливается для тяжелой электромагнитной обстановки. Примером условий, соответствующих степени жесткости 4, может служить электромагнитная обстановка силовых подстанций, коммутационного оборудования воздушных линий высокого напряжения, газонаполненных переключателей на напряжение до 500 кВ.

Степень жесткости 5 устанавливается для специальных условий эксплуатации технических средств по согласованию между потребителем и производителем.

Стандарт ГОСТ Р 50627 распространяется на технические средства, подключаемые к низковольтным электрическим сетям переменного однофазного или трехфазного тока частотой 50 Гц при токе нагрузки (в одной фазе) не более 16 А. Стандарт устанавливает степени жесткости испытаний и методы испытаний технических средств на устойчивость к воздействию динамических изменений напряжения сети электропитания вида провалов, прерываний и выбросов напряжения. Согласно этому стандарту, технические средства, подключаемые к электрическим сетям общего назначения, должны сохранять работоспособность при воздействии динамических изменений напряжения электропитания, вызываемых короткими замыканиями, внезапными изменениями нагрузки и процессами коммутации в электрических сетях. При проведении испытаний техническое средство должно функционировать непрерывно. Режим функционирования должен обеспечивать наибольшую восприимчивость к воздействию динамических изменений напряжения электропитания конкретного вида. Этот стандарт также определяет пять степеней жесткости испытаний оборудования, отличающихся от ГОСТ 29156.

При проведении испытаний по степеням жесткости 1 и 2 технические средства подключаются к электрическим сетям. В первом случае подключение производится к электрическим сетям с низким уровнем динамических изменений напряжения, характеризующимся практическим отсутствием прерываний и выбросов напряжений. Проверяется устойчивость только к провалам напряжения. Во втором случае — к рас-

пределительным электрическим сетям общего назначения со средним уровнем динамических изменений напряжения, характеризующимся возможностью появления провалов напряжения длительностью несколько десятков миллисекунд, прерываний и повышений напряжения длительностью от нескольких миллисекунд до нескольких десятков миллисекунд.

При проведении испытаний со степенью жесткости 3 технические средства подключаются к промышленным электрическим сетям с крайне неблагоприятной электромагнитной обстановкой, где может иметь место высокий уровень динамических изменений напряжения электропитания.

Степень жесткости 4 регламентирует подключение технических средств к промышленным электрическим сетям с крайне неблагоприятной электромагнитной обстановкой, где может иметь место высокий уровень динамических изменений напряжения электропитания. В этом случае желательно подвергать технические средства испытаниям на устойчивость ко всем видам динамических изменений напряжения электропитания со степенями жесткости 4 или устанавливать степень жесткости испытаний по согласованию между потребителем и производителем.

ГОСТ 30374-95/ГОСТ Р 50007-92 — еще один стандарт, устанавливающий технические требования к степени жесткости испытаний и методы испытаний на устойчивость к микросекундным импульсным помехам большой энергии, образуемым в цепях электропитания переходными процессами от молниевых разрядов и различного рода переключений.

В зависимости от условий эксплуатации технических средств, этот документ устанавливает технические требования для нескольких степеней жесткости. Согласно этим требованиям, технические средства должны сохранять работоспособность в условиях эксплуатации при воздействии на цепи электропитания микросекундных импульсных помех в виде молниевых разрядов и коммутационных переходных процессов.

В справочном приложении 2 этого стандарта приводится классификация условий эксплуатации технических средств. В зависимости от характеристик электромагнитной обстановки предлагаются семь классов условий эксплуатации: от нулевого до шестого. Степени жесткости испытаний применительно к классам условий эксплуатации технических средств представлены в табл. 2.5.

В отличие от предыдущих, рассматриваемый ниже стандарт ГОСТ 30375-95/ГОСТ Р 50008-92 регламентирует испытания, обеспечивающие защиту технических средств от высокочастотных помех. Согласно этому документу, технические средства долж-

Таблица 2.5. Степени жесткости испытаний применительно к классам условий эксплуатации технических средств

Класс условий эксплуатации	Степень жесткости испытаний при схеме передачи микросекундных импульсных помех	
	Провод-провод	Провод-земля
0	Не производятся	Не производятся
1	Не производятся	1
2	1	2
3	2	3
4	3	4
5	По согласованию между потребителем и заказчиком	
6		

ны сохранять заданное качество функционирования в условиях эксплуатации при воздействии электромагнитных полей, создаваемых стационарными радио- и телевизионными передатчиками, передвижными и переносными радиопередатчиками, промышленными, научными, медицинскими и бытовыми высокочастотными установками, портативными приемопередатчиками и другими источниками. Стандарт распространяется на те технические средства, которые могут в условиях эксплуатации подвергаться воздействию внешних радиочастотных электромагнитных полей в полосе частот 26—1000 МГц с регламентированными значениями параметров. Для испытаний технических средств в полосе частот 26—1000 МГц устанавливают степени жесткости испытаний, указанные в табл. 2.6.

Таблица 2.6. Степени жесткости испытаний технических средств в полосе частот 26—1000 МГц

Степень жесткости	Напряженность испытательного поля, дБ мкВ/м (В/м)
1	120(1)
2	130 (3)
3	140 (10)
4	По согласованию между потребителем и производителем

В отличие от рассмотренного выше, ГОСТ 29216—91 («Радиопомехи индустриальные от оборудования информационной техники. Нормы и методы испытаний») распространяется на оборудование информационной техники и устанавливает нормы и методы измерений индустриальных радиопомех в полосе частот 0,15—1000,0 МГц. По этому документу оборудование информационной техники подразделяют на два класса: А и В. К классу А относятся технические средства, которые эксплуатируют вне жилых зданий и не подключают к электросетям жилых зданий. Технические средства класса В эксплуатируют в жилых зданиях или подключают к электросетям этих зданий.

Как видно из приведенных выше документов, аппаратура информационных сетей с точки зрения сертификационных требований для 3 и 4 группы жесткости испытаний должна выдержать (данные для четвертой группы указаны в скобках):

- одиночный импульс по цепям питания, ввода/вывода и корпуса с амплитудой тока 30 А в начальный момент, длительность пика 0,7—1,0 нс, и далее 16 А в течение 60 нс (амплитуда импульса при контактном разряде емкости 6(8) кВ, а при воздушном разряде — 8(15) кВ);
- пачки импульсов через емкостную связь, каждый из которых имеет в начальный момент длительность пика 5 нс, общей длительностью до 50 нс (амплитуда импульса 2(4) кВ по цепям питания и корпуса и 1(2) кВ по цепям ввода/вывода и корпуса);
- не менее пяти импульсов с амплитудой 2(4) кВ через индуктивно-емкостную связь с длительностью фронта 1 мс и длительностью 50 мс по цепям питания и заземления.

Классификация воздействий основана на физике процессов и среды доставки энергетики. Малые по энергетике наносекундные воздействия получаются из статического разряда и коммутационных помех по коммуникациям. Сильные воздействия оказывают в основном грозовые разряды и переходные процессы, связанные с коммутацией

силовых цепей, особенно при срабатывании устройств защиты. К сожалению, это воздействие не рассматривается для кабельных информационных коммуникаций, а грозой «убита» не одна сотня видеокамер, модемов и прочего оборудования.

Выбор группы зависит от размещения технических средств (ТС) и их проводных коммуникаций. Компьютеры могут быть отнесены как к 3-й так и к 4-й группе жесткости, в зависимости от их назначения, производителя, наличия информационных коммуникаций. Домашний компьютер может быть отнесен ко 2-й группе, а что происходит в реальной жизни, к сожалению, неизвестно, особенно в случае закупки оборудования по принципу минимальной цены.

В случае с преднамеренными силовыми воздействиями не важна достоверность сертификата. Наоборот, он даже помогает определить необходимое силовое воздействие. Технология проста: берется класс исполнения технического средства, увеличивается в несколько раз энергетика (амплитуда, длительность и т. д.), по сравнению с указанными в ГОСТах, и можно атаковать противника. В этом случае для защиты техники нужно повысить класс устойчивости, добавить устройства защиты и не допускать «близких контактов», чтобы сделать максимально бессмысленным применение средств создания преднамеренных силовых воздействий по коммуникациям.

Деструктивные воздействия на компьютерные системы по цепям электропитания

В реальных условиях эксплуатации электронной аппаратуры в ее цепях питания возникают различного вида электрические перегрузки, создаваемые электромагнитными импульсами естественного и искусственного происхождения (грозовые разряды, статическое электричество, работа или авария другой электронной аппаратуры и электрооборудования, преднамеренные силовые воздействия по сетям обмена информацией и питания).

Любой компьютер или другое электронное оборудование информационно-вычислительных систем имеет источник питания. Без него аппаратура просто не может работать. Поэтому для деструктивного воздействия такой канал выбран не случайно.

Преднамеренное силовое воздействие по сети электропитания — это преднамеренное создание резкого всплеска напряжения в сети питания или (связи) с амплитудой, длительностью и энергией всплеска, способными привести к сбоям в работе оборудования или к его деградации (выводу из строя). Для этого используются специальные технические средства, которые подключаются к сети непосредственно с помощью гальванической связи, через конденсатор или трансформатор. В качестве примера такого средства можно привести так называемый «чемодан обнаружения» французской фирмы COFROEXPORT S.A., в состав которого входит подключаемый к сети питания высоковольтный генератор для вывода из строя несанкционированно подключенных к сети питания электронных систем.

По прогнозам специалистов, вероятность использования силового деструктивного воздействия будет расти год от года. Поэтому при разработке концепции безопасности необходимо учитывать и возможность таких воздействий по сетям питания, для чего, в первую очередь, необходимо провести классификацию технических средств силового воздействия. Возможная классификация современных технических средств силового деструктивного воздействия по сетям питания представлена на рис. 2.26.

К классу «Специальные и другие технические средства» отнесены, в частности, различные суррогатные средства деструктивного воздействия, имеющиеся под рукой. Например, может быть использована ближайшая трансформаторная подстанция, к части вторичной обмотки которой можно подключить техническое средство воздействия с емкостным накопителем, параметры которого подобраны так, что вторичная обмотка трансформатора, магнитопровод и емкостной накопитель образуют повышающий резонансный автотрансформатор. Такое силовое воздействие может вывести из строя все электронное оборудование, обслуживаемое данной подстанцией.

К этому же классу отнесены и средства перепрограммирования источников бесперебойного питания (UPS) с использованием, например, программных закладок. Современные мощные полнопроточные UPS импортного производства имеют встроенное программное обеспечение для управления, в том числе и уровнем выходного напряжения. Соответствующая программная закладка может быть активизирована в любой момент командой по сети электропитания и на короткое время перепрограммирует UPS на максимально возможное выходное напряжение, которое приведет к выходу из строя защищаемого UPS оборудования. Поскольку программное обеспечение UPS специализировано, искать такие закладки трудно.

В качестве примера относительно недорогих устройств деструктивного воздействия можно привести устройства с электролитическими конденсаторами, имеющие удельную объемную энергию, равную 2000 кДж/м^3. Подобное устройство, размещенное в обычном кейсе, способно вывести из строя до 20-и компьютеров одновременно. Ориентировочная стоимость такого кейса составляет от 10 000 до 15 000 долларов США.

Еще эффективнее работают молекулярные накопители (ионисторы), удельная объемная энергия которых достигает 10 МДж/м^3. Технические средства деструктивного воздействия, содержащее ионисторы, способны вывести из строя все компьютеры даже большого вычислительного центра. Стоит такое техническое средство примерно 50 000 долларов США.

Рис. 2.26. Классификация технических средств силового деструктивного воздействия по сетям питания

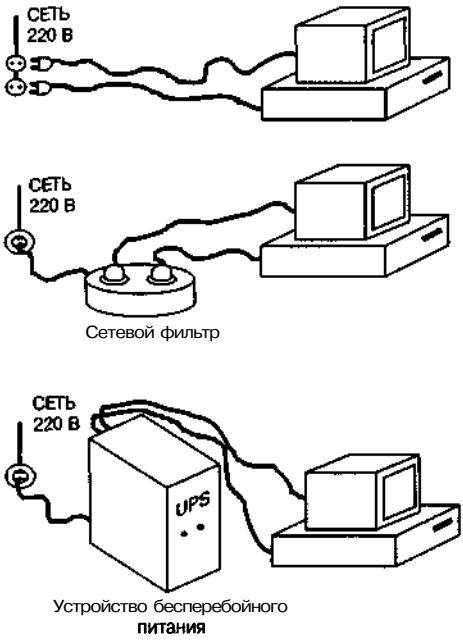


Рис. 2.27. Варианты питания компьютеров от сети

Чтобы понять, как могут злоумышленники воздействовать на отдельные компьютеры и на информационные системы в целом, рассмотрим обычные варианты питания компьютера от электрической сети (рис. 2.27).

Первый вариант самый простой, самый дешевый и потому самый распространенный. Не используются никакие дополнительные устройства, компьютер подключается непосредственно к силовой сети. Так подключены большинство домашних компьютеров. Ни сам компьютер, ни его монитор в этом случае не защищены от деструктивных воздействий, независимо от того, преднамеренно или непреднамеренно они происходят.

Во втором варианте подключения к сети используется сетевой фильтр. Сетевые фильтры предназначены для защиты цепей электропитания компьютеров, периферии и другой электронной аппаратуры от:

- О импульсных перенапряжений и выбросов тока, возникающих в результате коммутации и работы промышленного оборудования;
- ❑ высокочастотных помех, распространяющихся по сетям электропитания;
- ❑ импульсных перенапряжений, возникающих в результате грозовых разрядов.

Третий вариант отличается от предыдущих наличием устройства бесперебойного питания, которое позволяет корректно завершить работы на компьютере при пропадании сетевого питания.

Существуют и другие варианты подключения: например, с использованием специальных генераторов. Их мы рассматривать не будем ввиду экзотичности и малого распространения.

Итак, начнем с рассмотрения первого варианта. В этом случае блок питания компьютера непосредственно подключен к сети и для проникновения энергии силового воздействия по сети питания есть два пути:

- ❑ **кондуктивный** путь через источник вторичного электропитания;
- ❑ наводки через паразитные емкостные и индуктивные связи, как внутренние, так и между совместно проложенными силовыми кабелями и информационными линиямисвязи.

Современный блок питания компьютера — это сложное многокаскадное устройство, в котором стабилизированное напряжение вырабатывается после ряда преобразований. Чтобы понять, как можно преднамеренно воздействовать на компьютер по сетям питания, рассмотрим структурную схему блока питания компьютера мощностью 200 Вт, изображенную на рис. 2.28.

Входное напряжение (115 или 230 В переменного тока) поступает на сетевой фильтр, состоящий обычно из нескольких индуктивностей, конденсаторов небольшой емкости и разрядного резистора. Далее питающее напряжение поступает на высоковольтный выпрямитель, который конструктивно представляет собой 4 диода, включенные по мостовой схеме и обычно помещенные в общий пластмассовый корпус. Выпрямленное напряжение поступает на высоковольтный фильтр, представляющий собой два электролитических конденсатора емкостью 200—500 мкФ.

Отфильтрованное постоянное напряжение поступает на высоковольтный транзисторный ключ, собранный по одно- или двухтактной схеме, который переключается схемой управления с частотой в несколько десятков килогерц. Импульсы напряжения поступают на импульсный понижающий трансформатор, который выдает на вторичных обмотках напряжения для каналов +5 , +12 , —5 и —12 В.

Согласно этой структурной схеме, приведем примерную принципиальную схему блока питания компьютера (рис. 2.29) и рассмотрим ее возможности по защите от силовых деструктивных воздействий.

Для оценки устойчивости этого блока питания к преднамеренным силовым воздействиям достаточно оценить предельную энергопоглощающую способность и электрическую прочность ряда элементов схемы и сопоставить ее в дальнейшем с энергией и выходным напряжением атакующих технических средств.

Подавление импульсных помех на пути из сети питания к чувствительным микросхемам происходит во входных цепях блока питания, главным образом — во входном фильтре. Этот же узел первым принимает на себя удар преднамеренного силового воздействия по сети питания. На самом деле элементы входного LC-фильтра имеют чрезвычайно низкие уровни предельной энергопоглощающей способности и не являются препятствием на пути мощных импульсных помех. Это вполне объяснимо, так как LC-фильтр в основном предназначен для решения обратной задачи: он препят-

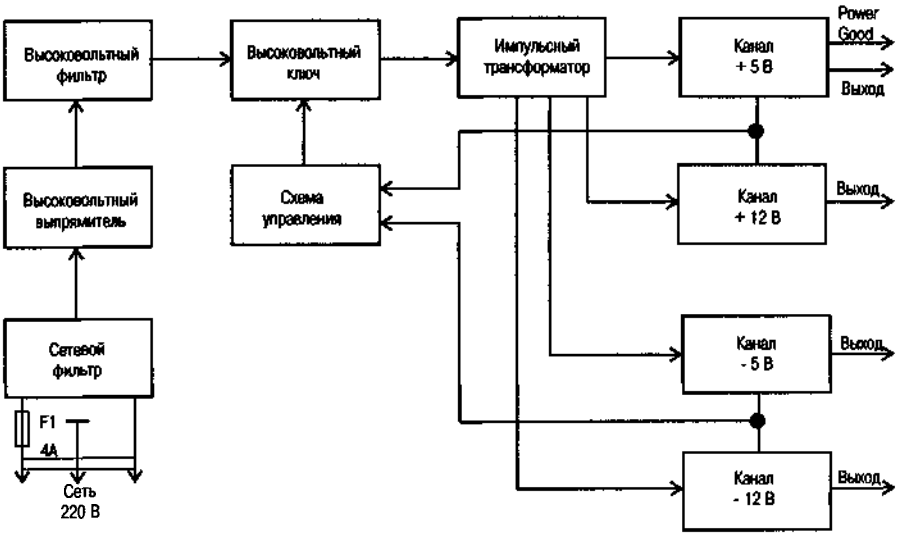


Рис. 2.28. Структурная схема блока питания компьютера

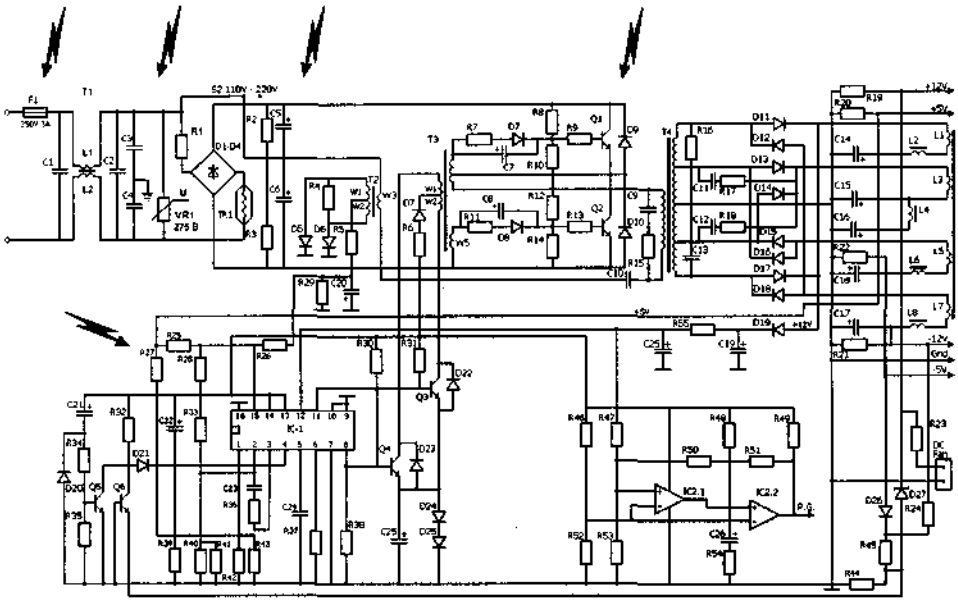


Рис. 2.29. Принципиальная схема блока питания

ствует распространению в сеть питания собственных шумов, создаваемых при работе элементов блока питания. Уровень этих шумов составляет доли вольта, и поэтому при проектировании фильтра предельная энергопоглощающая способность его элементов не является определяющим фактором. Дроссели фильтра характеризуются прочностью изоляции между катушками, которая обыкновенно не превышает 2500 В.

Если LC-фильтр — это единственное устройство защиты на входе источника питания (именно так устроено большинство дешевых блоков питания компьютеров), то для успешного силового воздействия достаточно обеспечить возможность подвода к каждому атакуемому компьютеру мощной импульсной помехи с амплитудой порядка 2 кВ и энергией 1—2Дж с достаточно крутым фронтом, уменьшающим влияние емкостного фильтра инвертора блока питания.

Конденсаторы на входе источника питания имеют рабочее напряжение 250 В для переменного и 1000 В для постоянного напряжения. Они обладают до момента пробоя энергопоглощающей способностью 300 мДж. При испытаниях компьютеров в соответствии с упомянутыми в начале этого раздела российскими стандартами (равно как и при испытаниях по IEEE Standard 587-1980 и аналогичным западным стандартам) амплитуда импульса испытательного напряжения намного больше, но длительность составляет лишь 20 мкс, поэтому конденсаторы не успевают зарядиться до напряжения пробоя. Это означает, что тестирование компьютера по самым жестким нашим и западным стандартам не гарантирует его устойчивости к преднамеренным силовым воздействиям, так как эти стандарты ориентированы на коммутационные помехи и индуцированные разрядом молнии напряжения, но не на искусственно создаваемые помехи.

Основные функции защиты от мощных импульсных помех в качественных источниках питания выполняет варистор. Варистор начинает работать при напряжении порядка 500—600 В и ограничивает амплитуду импульсного напряжения на уровне 710 В при токе импульса помехи 10/25/50/100 А, при больших же токах амплитуда остаточного напряжения много выше.

Сказанное относится к варисторам с классификационным напряжением 275 В, однако в большинстве источников питания и дополнительных устройствах защиты типа ограничителей установлены варисторы с классификационным напряжением 420 или 460 В, а они ограничивают напряжение на уровне 1100—1240 В при малых токах, для больших токов эти значения много выше. Быстродействие варистора составляет 25 нс, поэтому от наносекундных импульсных помех он оборудование не защищает.

Несмотря на впечатляющие уровни рабочих токов, варисторы имеют предельно допустимую рассеиваемую мощность в единицы ватт, поэтому при воздействии длинных импульсов с относительно небольшим током они выходят из строя или срабатывают, в результате чего сгорает предохранитель на входе источника питания. Возникает необходимость ремонтировать весь блок, и объект атаки — компьютер — на время выводится из строя. Тем не менее, в данном случае для успешной атаки техническим средствам силового воздействия требуется энергия порядка 50—100 Дж при амплитуде порядка 1 кВ (причем длительность импульса может доходить до 0,1 с для инерционных предохранителей) в расчете на один атакуемый компьютер, а их одновременно подключено к сети питания может быть много. Учитывая, что существенная доля энергии при этом может передаваться не на вход конкретного источника питания, а в общую сеть (до ближайшей трансформаторной подстанции), конструкция атакующих средств усложняется, возрастают габариты и требуется более серьезное вмешательство в сеть питания объекта атаки для их подключения.

Значительно меньше энергии требуется для повреждения конденсаторов входного фильтра инвертора и диодов выпрямительного моста. Конденсаторы входного фильтра инвертора имеют предельную энергопоглощающую способность равную 10—15 Дж при суммарном напряжении пробоя 480—500 В. Длительность импульса, при котором пробивается изоляция конденсаторов, должна быть не менее 0,5 мс с учетом сопротивления термистора TR1. Допустимое значение обратного напряжения для диодов составляет 600—1000 В, допустимая амплитуда однократного импульса тока 60/100/200 А для диодных сборок на номинальный ток 2/3/4 А, предельная энергопоглощающая способность менее 1 Дж. Пробивные напряжения транзисторов инвертора обыкновенно не превышают значений 500—800 В, а предельная энергопоглощающая способность менее 1 Дж.

При этом технические средства силового воздействия генерируют импульс, «обходящий» варисторную схему защиты. Для этого используется разница напряжения пробоя конденсаторов и напряжения, при котором наступает эффективное ограничение напряжения варистором (оно больше напряжения пробоя конденсаторов на 70—120 В). В пересчете на один атакуемый компьютер техническому средству силового воздействия достаточно выдавать в сеть энергию порядка 15—25 Дж при амплитуде импульса 500—600 В и длительности до 5 мс. После пробоя конденсаторов дополнительно возникает импульс тока через диоды моста, который при горячем термисторе доходит до 1000 А, повреждая диоды. Для большинства блоков питания при таком

воздействии весьма вероятен выход из строя транзисторов и других элементов инвертора, а также выбросы напряжения на выходе источника питания, приводящие к поломке других узлов компьютера. Результаты оценки устойчивости элементов типового блока вторичного источника питания компьютера приведены в табл. 2.7.

Таблица 2.7. Результаты оценки устойчивости элементов источников питания к силовому деструктивному воздействию

Обозначение элемента	Тип элемента	Энергопоглощающая способность, Дж	Предельная поглощающая способность, Дж	Прочность изоляции, в	Примечание
C1, C2	Конденсатор	0,3		1200	Рабочее напряжение: 250 В — переменное, 1000 В — постоянное
L1, L2	Дроссель	0,1		2500	Главное — изоляция между катушками
C3, C4	Конденсатор	0,002		1200	
VR1	Варистор	20/ 40/ 70/ 140 соответственно для диаметра 7/10/14/20 мм	$(3–4000) \times 10^{-3}$		Быстродействие 25 нс, от наносекундных помех оборудование не защищает
VD1-VD4	Полупроводниковый диод	Менее 1	$(0,1–1000) \times 10^{-3}$	600–1000	Допустимая амплитуда импульса тока 60/100/200 А для микросборок на 2/3/4 А
Q1, Q2	Транзистор	Менее 1	$(20–1000) \times 10^{-3}$	500–800	
C5, C6	Конденсатор	15		500	Изоляция может быть пробита при длительности импульса не менее 0,5 мс

Электрическая прочность изоляторов конденсаторов, изоляционных барьеров, дросселей, проводов, коммутационных изделий и пр. нормируется для постоянного тока либо для рабочих частот (как правило, 50 или 400 Гц), и это имеет слабое отношение к обсуждаемой теме, хотя для импульсных воздействий электрическая прочность (если технически вообще правомерно подобное высказывание по отношению к импульсным перенапряжениям) значительно ниже, поэтому и требуется применение элементов активной защиты.

Аппаратная часть компьютера за блоком питания весьма чувствительна к воздействию импульсных помех. Чем выше полупроводниковая технология аппаратуры, тем более техника подвержена разрушению. Сбой в работе цифровых микросхем возникает при появлении на шине питания импульса с амплитудой в единицы вольт при длительности в десятки наносекунд. Деградация цифровых микросхем наступает при воздействии импульсов напряжения длительностью 1 мкс с энергией 2—500 кДж.

Минимальная энергия, вызывающая функциональные повреждения полупроводниковых приборов и интегральных микросхем, определяется критической энергией, разрушающей полупроводниковый переход (электрическая прочность полупроводникового перехода). Эта энергия достаточно мала и порой составляет 10-2-10-7Дж, к тому же она не зависит от параметров импульсного воздействия и определяется только физико-конструктивными параметрами полупроводникового перехода.

Между соединительными проводниками или элементами схемы, а также между ними и корпусом или экранирующей шиной всегда имеются емкость и индуктивность монтажа. Их можно рассматривать как возможные пути распространения импульсов силового воздействия на элементы технических средств. На рис. 2.30 представлены эквивалентные схемы емкостного и индуктивного путей распространения помехи.

В качестве примера одного из видов воздействия можно рассмотреть влияние металлической подложки гибридной микросхемы на помехоустойчивость схемы управления блока питания (рис. 2.31, а). Другой случай негативного влияния паразитной емкости монтажа можно проиллюстрировать на примере межобмоточной емкости силового трансформатора блока питания (рис. 2.31, б).

Как видно из рис. 2.31, входные высоковольтные и выходные низковольтные цепи источников питания компьютеров имеют емкостную связь через паразитную емкость, величина которой может составлять 10—30 пФ. Такая величина обусловлена тем, что в подавляющем большинстве компьютерных источников питания сложно реализовать специфические требования, предъявляемые к конструкции фильтров НЧ (разбивку корпуса на экранированные отсеки, применение элементов с малой собственной емкостью/индуктивностью, оптимальную трассировку монтажных жгутов и т. п.).

Если прокладка кабеля к сетевому выключателю внутри корпуса компьютера выполняется без учета требований электромагнитной совместимости, то появляется паразитная емкость величиной 5—10 пФ, связывающая сеть питания с элементами материнской платы.

Если атакующие средства используются для провоцирования сбоев в работе информационной системы, то они генерируют высоковольтные импульсы с наносекундным временем нарастания. Для таких импульсов импеданс паразитных емкостей составляет доли ома, поэтому энергия импульсов эффективно передается как на шины питания узлов информационной системы в виде импульсов напряжения, так и во внут-

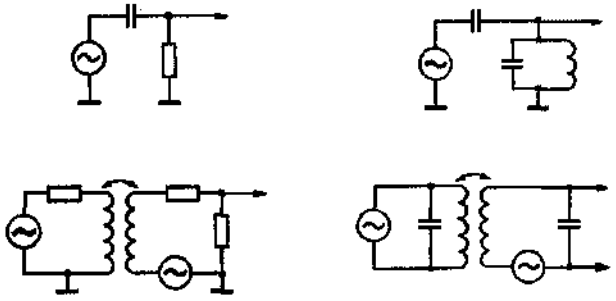


Рис. 2.30. Эквивалентные схемы емкостного и индуктивного путей распространения помехи

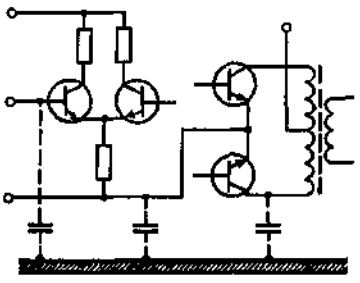


Рис. 2.31. Примеры путей распространения импульсных помех

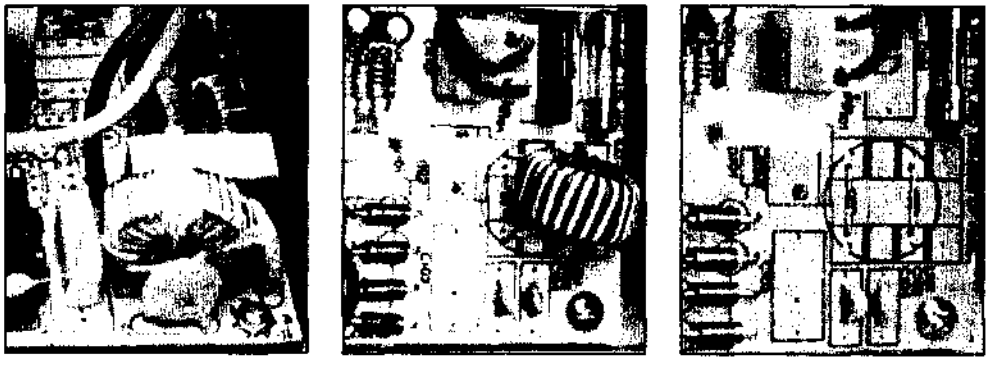
ренние объемы корпусов компьютеров и другого оборудования в виде импульсных электромагнитных полей. Импульсные воздействия короче 100 нс не требуют мощной энергетики и достаточно просто достигают своей цели, проходя к ней по паразитным емкостям, следствием этого является «зависание» компьютеров, сбои в работе программного обеспечения, искажение данных.

Мы рассмотрели, как может быть атакован блок питания компьютера, выпущенный известным производителем и протестированный соответствующим образом. Однако часто при покупке компьютера в первую очередь выбирают хороший процессор, винчестер, а на корпусе — и, соответственно, на блоке питания — предпочитают экономить и приобрести так называемый no-name.

Ради копеечной экономии некоторые производители блоков питания, не моргнув глазом, идут на прямые нарушения международных стандартов. Нарушений встречается очень много, но меньше всего можно предположить, что в таком ответственном приборе, как блок питания, забудут припаять какую-нибудь деталь. А такое происходит довольно часто, и в большинстве случаев виной тому даже не рассеянность монтажников. На рис. 2.32 показаны варианты, продаваемых блоков питания с различными изменениями во входном фильтре импульсных помех.

Если такого фильтра нет или его параметры не отвечают определенным требованиям, то блок питания не пройдет сертификацию и его нельзя продавать. Но для нашего рынка «нельзя продавать» вовсе не означает «не продается».

Кроме того, в низкокачественных источниках питания, как правило, отсутствуют некоторые элементы цепей защиты (чаще всего — варисторы и термисторы) и/или использованы более дешевые элементы: конденсаторы с меньшей емкостью, варисто-



Питание подведено после фильтра

Отсутствуют конденсаторы фильтра

Фильтр отсутствует, стоят перемычки

Рис. 2.32. Варианты исполнения фильтров блока питания

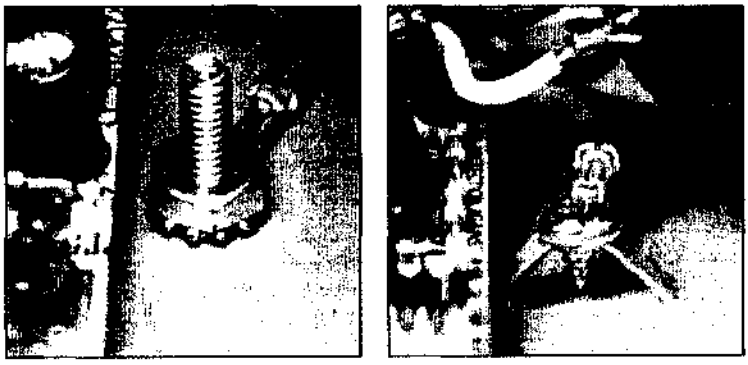
ры с меньшей энергией, вместо термисторов — обычные резисторы. О защите от силового воздействия в этих случаях вообще говорить не приходится.

Необходимая защита сводится к нулю из-за особенностей некоторых корпусов компьютеров или примененных разъемов. Пробой по поверхности изолятора (или по воздуху) по цепи кабель—корпус компьютера прогнозируем — по поверхности изолятора 1 кВ/3 мм и 1 кВ/1 мм по воздуху. Атакующее средство, которое воздействовало бы на электросеть (или контур заземления) и подключенный коаксиальный кабель, сделать достаточно просто. Подобные разряды создают достаточное возмущение для разрушения, причем защита по сети источника даже помогает в этом.

Различная периферия, подключенная к незащищенным цепям и питающаяся от незащищенных источников, — внешние модемы, активные колонки, некоторые принтеры, сканеры — может служить (а так обычно и бывает) для прохождения силовых воздействий в информационную систему.

Даже тип сетевого включателя компьютера может оказать влияние на устойчивость информационной системы по отношению к силовому воздействию. Если, например, в конструкции источника питания (или устройства, его содержащего) используется однополюсный сетевой выключатель, то при подаче в цепь между одним из проводов питания и шиной заземления импульса напряжения с амплитудой 3—4 кВ и энергией 1—2 Дж произойдет следующее. Через замкнутый контакт выключателя, находящийся в положении «выключено», энергия импульса попадет на элементы источника питания и приведет к пробою изоляции на корпус. Несмотря на примитивность такого метода атаки, его можно использовать ради маскирующего эффекта. Если силовое воздействие проводится ночью, то при включении компьютера оператор может обнаружить нарушение его работоспособности и отнести это на счет переходных процессов при включении.

Неправильно выполненное защитное заземление может не только стать «лазейкой» для силового воздействия, но и поставить под угрозу человеческую жизнь. Пример исполнения соединения провода защитного заземления с корпусом блока питания представлен на рис. 2.33.



Правильно Неправильно

Рис. 2.33. Выполнение заземления

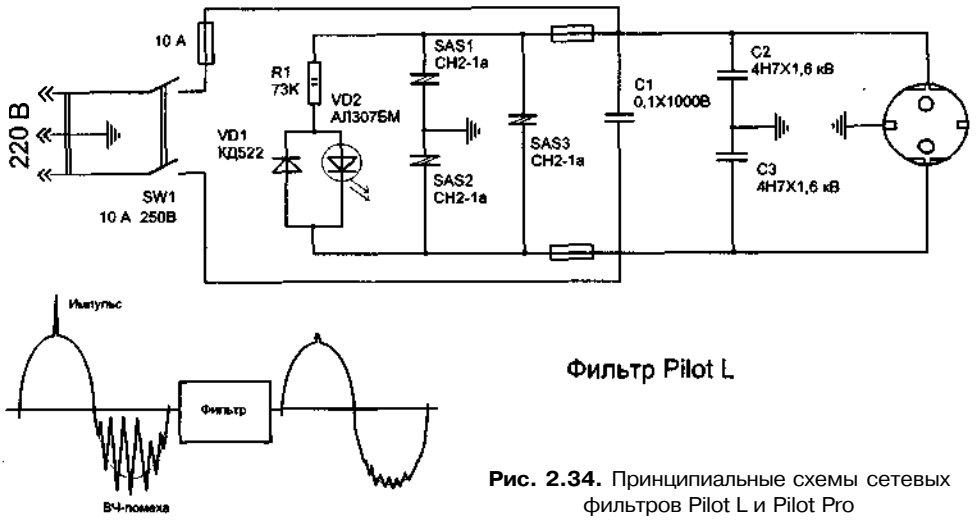


Рис. 2.34. Принципиальные схемы сетевых фильтров Pilot L и Pilot Pro

Для правильного выполнения заземления обязательно необходим болт, клемма заземления должна быть привинчена гайкой с пружинной шайбой. Вид самореза, ввинченного без шайб в непонятную «фитюльку», вызывает только сочувствие к обладателю такого блока. Этот недостаток можно легко обнаружить, если снять крышку блока питания. Но обычно его продают опломбированным и грозят лишить гарантии, если покупатель окажется слишком любопытным и захочет заглянуть под эту крышку.

Второй способ подключения компьютера к питающей сети — через сетевой фильтр — практически не отличается от рассмотренного выше. При поломке сетевого фильтра может произойти потеря данных или выход из строя самого компьютера. Принципиальные схемы сетевых фильтров Pilot L, Pilot Pro представлены на рис. 2.34, а их технические характеристики — в табл. 2.8. Как видно на принципиальных схемах, простые сетевые фильтры выполняются практически так же, как и входные фильтры источников питания.

Таблица 2.8. Технические характеристики сетевых фильтров

Характеристика	Модель	
	Pilot L	Pilot Pro
Номинальное напряжение/частота, В/Гц	220 В/50-60	220 В/50-60
Суммарная мощность нагрузки, кВт	2,2	2,2
Номинальный ток нагрузки, А	10	10
Ослабление импульсных помех, раз импульсы 4 кВ, 5/50 нс импульсы 4 кВ, 1/50 мкс	 Не менее 10 Не менее 4	 Не менее 30 Не менее 6
Ток помехи, выдерживаемый ограничителем, кА	Не менее 2.5	Не менее 8
Максимальная поглощаемая энергия, Дж	80	300
Уровень ограничения напряжения при токе помехи 100 А, В	700	600
Ослабление высокочастотных помех, дБ 0,1 МГц 1 МГц 10 МГц	 5 10 30	 20 40 20
Потребляемая мощность(не более), ВА	2	15

Как правило, сетевые фильтры защищают только от больших перепадов напряжения. Во многих конструкциях защитные свойства сетевого фильтра базируются на использовании в электрической схеме мощных нелинейных резисторов — варисторов. При нормальном напряжении ток через варистор практически не течет. В момент броска напряжения сопротивление варистора резко уменьшается, через варистор течет ток. Другими словами, варистор шунтирует цепь питания компьютера, телевизора и т. д., рассеивая энергию импульса на себе.

Для третьего варианта подключения компьютера к сети характерно включение между сетью и блоком питания дополнительного устройства защиты. Обычно для этих целей используются устройства бесперебойного питания (UPS), которые предназначены для улучшения качества электроэнергии сети переменного тока и обеспечения бесперебойного электропитания оборудования при выходе ее из строя. Существуют устройства бесперебойного питания нескольких основных типов, но все они обязательно содержат следующие функциональные узлы:

- ❑ входной фильтр-ограничитель перенапряжений;
- О зарядное устройство для аккумуляторов;
- ❑ аккумуляторный блок;
- ❑ преобразователь напряжения или инвертор;
- О переключатель каналов;
- ❑ стабилизирующий каскад;
- ❑ система управления.

Источники бесперебойного питания различают по классам (режимам работы):

- ❑ off-line (stand-by);
- ❑ on-line;
- ❑ гибридные (line interactive).

Главное различие заключается в выборе основного канала передачи энергии к потребителю. Для класса off-line в каждый момент времени UPS может находиться в одном из двух режимов работы — stand-by или on-line. В основном режиме, когда напряжение в сети находится в допустимых пределах (standby mode), компьютер запитывается через ветвь, содержащую только входной фильтр (рис. 2.35). При этом аккумуляторы подзаряжаются от маломощного зарядного UPS, а напряжение с инвертора не поступает на выход источника. В этом режиме функционирование UPS ничем не отличается от работы обыкновенного сетевого фильтра. Никакой стабилизации напряжения не происходит.

Поскольку питание компьютера и периферийного оборудования обеспечивается напряжением промышленной сети переменного тока, постоянное напряжение акку-

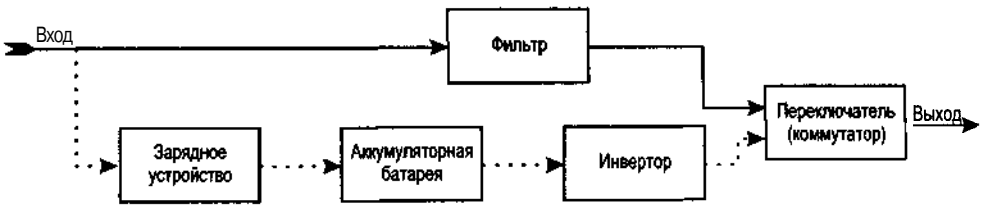


Рис. 2.35. Структурные схемы UPS типа off-line (а), on-line (б), line interactive (в)

муляторной батареи должно быть преобразовано в переменное, соответствующее номинальному напряжению сети. Для этого в UPS используется специальное устройство — инвертор.

Если подача электроэнергии прекратилась или напряжение в сети стало ниже некоторой допустимой величины, то UPS подключает питание от батарей и ветвь, содержащую инвертор, тогда энергия к потребителю поступает от аккумуляторов.

Среди достоинств UPS off-line стоит отметить простоту схемного решения, дешевизну, минимальные габариты и небольшой вес. Эти источники целесообразно использовать для защиты персональных компьютеров, периферийного оборудования, бытовой оргтехники.

Особенность данной системы в том, что переключение в on-line при выходе напряжения сети за допустимые пределы происходит очень быстро, а возврат в standby mode — с обязательной задержкой в несколько секунд. Иначе, при многократных бросках напряжения в сети, происходило бы непрерывное переключение stand-by/on-line и обратно, что привело бы к значительным искажениям тока нагрузки и возможному выходу ее из строя или к сбою в ее работе.

Недостаток подобных устройств — наличие времени переключения и отсутствие стабилизации выходного напряжения при работе от сети. Время переключения — это время реакции UPS на пропадание или уменьшение/превышение напряжения сети. Что бы ни писали производители UPS, это время реально не может быть меньше 10 мс — один полупериод 50 Гц сети. В большинстве случаев это время составляет полный период — 20 мс. Когда производитель пишет, что время переключения 1 или 2 мс, то имеется в виду скорость срабатывания переключателя (коммутатора). Но ведь прибору надо «определить», что напряжение пропало, и «принять решение» переключаться, а это невозможно сделать за 1 мс, ибо подобный анализ привязан к самой длительности периода переменного напряжения. В результате реальная скорость переключения зачастую определяется именно временем анализа состояния сети. Этого времени оказывается достаточно, чтобы короткие импульсы силового воздействия достигли цели.

Класс устройств бесперебойного питания типа on-line характеризуется постоянством включения ветви, содержащей мощное зарядное устройство, аккумулятор и инвертор на выходе блока. Иными словами, в устройствах on-line отсутствует проблема переключения, т. к. в них преобразование идет всегда. Подобная схема позволяет обеспечить гальваническую развязку вход/выход стабильного синусоидального выходного напряжения. При выходе из строя какого-либо каскада в прямой ветви передачи энергии, перегрузках, а также при разряде аккумуляторов, переключатель каналов подключает ветвь, соединяющую вход-выход через фильтр. Этот вспомогательный путь передачи энергии, получивший название байпас, имеет особое значение при силовом деструктивном воздействии, поскольку позволяет обойти защиту устройства бесперебойного питания для поражения более важных блоков компьютерной системы (например, блок питания компьютера).

Устройства бесперебойного питания типа on-line называют еще источниками с двойным преобразованием или кондиционером сети. В них входное переменное напряжение с помощью выпрямителя преобразуется в постоянное и поступает на высокочастотный преобразователь (рис. 2.36). С выхода этого преобразователя напряжение

высокой частоты поступает на инвертор и с него — на выход устройства. Необходимость применения ВЧ-преобразователя обусловлена тем, что значительные изменения напряжения сети преобразуются в относительно небольшие изменения напряжения частоты ВЧ-сигнала на его выходе. Дело в том, что электроника компьютера более критична к изменению уровня питающего сетевого напряжения, чем к его частоте.

Источники бесперебойного питания архитектуры on-line стоят дороже и применяются, когда необходима надежная защита жизненно важного оборудования, часто работающего круглосуточно (серверы сетей, медицинское оборудование, персональные компьютеры, выполняющие особо важные функции и т. п.).

Реальные конструкции UPS по схеме on-line должны, в принципе, защищать подключенное к ним оборудование от силовых деструктивных воздействий, но этой защиты они все-таки не обеспечивают. Прежде всего, UPS имеет схему питания собственных нужд, которая содержит импульсный источник питания, аналогичный компьютерному, поэтому при силовом воздействии по сети питания UPS выходит из строя, причем обычно срабатывает байпас, и через него энергия силового воздействия от специальных технических средств беспрепятственно достигает цели в обход UPS.

У мощных полнопроточных UPS, помимо механического, имеется электронный (тиристорный) байпас. Его паразитная емкость достигает нескольких тысяч пикофарад, поэтому короткие импульсы с крутым фронтом проходят через нее в обход UPS совершенно беспрепятственно.

Рекламируемые низкая проходная емкость самого UPS (порою сообщается о единицах пикофарад) и ослабление помех на 120-130 дБ на практике оказываются всего лишь рекламой. Короткие импульсы длительностью в несколько миллисекунд через паразитные емкости не проходят. Но если на эти импульсы в атакующих технических средствах накладываются короткие высоковольтные, которые предварительно отпирают по аноду тиристоры электронных байпасов, то возникает путь для пропуска основной энергии к атакуемой цели.

Устройства бесперебойного питания гибридной архитектуры (line interactive) являются, по существу, усовершенствованием UPS типа off-line. У таких источников (рис. 2.37) инвертор подключен к выходу постоянно и не происходит переключений режима его работы при аварии питающего напряжения сети.

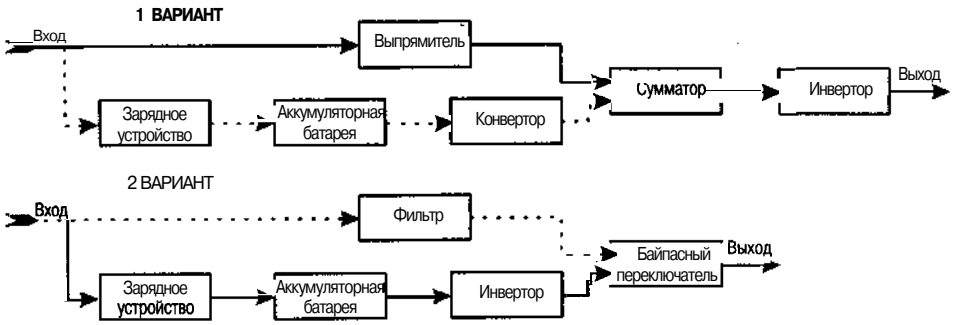


Рис. 2.36. Структурная схема UPS типа on-line

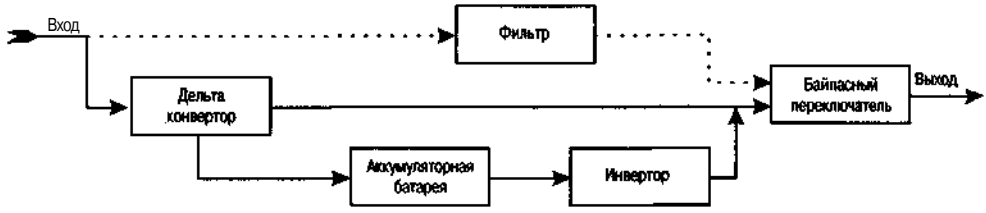


Рис. 2.37. Структурная схема UPS типа line interactive

На базе рассмотренных структурных схем UPS в настоящее время реализуются малогабаритные источники бесперебойного питания с интеллектуальной схемой управления, способные плавно регулировать напряжение на выходе и отлично изолировать нагрузку от шумов, импульсов и искажения синусоиды.

Устройства, выполненные по новой технологии, работают с использованием двух независимых инверторов.

Первый инвертор (delta converter) обычно рассчитан примерно на 20% от выходной мощности UPS и через трансформатор соединен последовательно с цепью питания нагрузки от электросети. Будучи синхронизированным с электросетью по частоте и фазе, он добавляет к сетевому или вычитает вырабатываемое им напряжение (delta voltage), тем самым компенсируя отклонения выходного напряжения от номинала. Кроме того, на delta converter возложены также функции PFC (Power Factor Correction) и управления зарядом батарей.

Второй инвертор рассчитан на 100%-ю выходную мощность UPS и предназначен для питания нагрузки при работе от батарей. Байпасный переключатель, как и в предыдущей топологии, обеспечивает непосредственное питание нагрузки от электросети в случае неисправности UPS или его временного отключения при плановом обслуживании.

Проанализировав рассмотренный материал, можно сделать вывод, что традиционные устройства защиты питания информационных сетей не только не защищают их от силового деструктивного воздействия, но и сами им подвержены.

Практически любые стабилизаторы и кондиционеры напряжения, предлагаемые для защиты компьютеров, обеспечивают лишь слабую защиту нагрузки и питания собственных нужд от импульсных помех, а предельно допустимое напряжение питающей сети (220/230 В + 10/-20%) много ниже требуемого для защиты от силовых воздействий (220 В +40-70%). В тиристорных стабилизаторах, корректорах напряжения, переключателях сети при воздействии на них с помощью специальных технических средств, вопреки штатному алгоритму схемы управления с аварийным отключением или выходом из строя, происходит самопроизвольное отпирание тиристоров байпаса. Устройства же, ориентированные на защиту от силового воздействия, должны использовать схемотехнику, направленную на подавление мощных импульсных помех, мощных радиопомех, перенапряжений в значительном диапазоне и, кроме того, они должны содержать дополнительные узлы, построенные с учетом специфических особенностей технических средств силового деструктивного воздействия.

Современные устройства активной защиты от перенапряжений не квалифицируются по природе воздействий; не столь важно, что на них воздействует — гроза, коммутация, статический разряд или средство создания преднамеренного силового воздействия.

Таблица 2.9. Защита информационных систем от силового деструктивного воздействия по сети питания

Действие	Особенности
На все фидеры, выходящие за пределы контролируемой службой безопасности зоны, установить групповые устройства защиты от силового деструктивного воздействия	Групповые устройства защиты установить в зонах, подконтрольных службе безопасности
На сеть электропитания серверов, систем охраны и сигнализации объекта установить индивидуальную защиту	В зависимости от решаемых задач объем индивидуальной защиты может быть существенно расширен
Щитки питания, распределительные щиты, розетки, клеммы заземления и т. п. необходимо размещать в помещениях, контролируемых службой безопасности	Не рекомендуется установка розеток в слабо контролируемых помещениях (буфет, склад, гардероб и т. п.)
Используя анализатор неоднородности линии, снять контрольный «слепок» электросети	Контрольный «слепок» снимается после завершения монтажа сети
Для выявления несанкционированного подключения к сети необходимо регулярно проверять текущий «слепок» и сравнивать его с контрольным «слепком»	Этот метод контроля особенно эффективен для обнаружения технических средств силового деструктивного воздействия последовательного типа
Доступ к щитам питания и другим элементам электрооборудования должен быть ограничен	Ограничение определяется соответствующими документами и мероприятиями
Все электрооборудование, в том числе и бытового назначения, следует тщательно проверять	Особое внимание обратить на устройства бесперебойного питания, микроволновые печи, пылесосы, кондиционеры, аппараты для сварки
Организовать круглосуточный мониторинг сети электропитания, одновременно записывая в журнал все сбои и повреждения оборудования, фиксируя время сбоев и характер дефектов; путем анализа результатов возможно своевременное обнаружение факта НСД	В качестве регистраторов можно использовать широкий спектр приборов: от простых счетчиков импульсов до компьютеризованных комплексов
При закупке электрооборудования необходимо обращать внимание на степень его защиты от импульсных помех; обычное оборудование должно иметь класс устойчивости не ниже А, ответственное — не ниже В	По стандарту IEEE 587-1980 помеха класса А: 0,5 мкс/6 кВ/200 А/1,6 Дж; класса В: 0,5 мкс/6 кВ/500 А/4 Дж
Для защиты 1-го рубежа лучше всего подходят специально разработанные помехозащищенные трансформаторные подстанции и суперфильтры; класс защиты должен быть выше В, т. е. устройство защиты должно быть рассчитано на воздействие индуцированных напряжений от близких разрядов молний с возможным импульсным током до 40 кА	Автоматические устройства переключения сети не защищают от силового деструктивного воздействия из-за низкого быстродействия; также малопригодны тиристорные стабилизаторы и корректоры
Для защиты 2-го рубежа могут использоваться технические средства с меньшим запасом энергии, в том числе суперфильтры, корректоры напряжения и помехоподавпяющие трансформаторы	Суперфильтры, помимо специальных фильтров и ограничителей напряжения, могут содержать адаптивные схемы поглощения энергии силовых воздействий
Для защиты 3-го рубежа наиболее подходят помехоподавляющие трансформаторы (трансфильтры) или сочетание корректора напряжения, ограничителя и фильтра; трансфильтр гораздо эффективней остальных типов фильтров и корректоров напряжения	Современные конструкции трансфильтров обеспечивают работоспособность компьютера при воздействии мощной импульсной помехи с амплитудой до 10 кВ

Защита от любых преднамеренных силовых воздействий, достаточно упрощенно, состоит из двух этапов: выявление путей воздействий и их закрытие. Как вы справитесь с первой частью, так же эффективна будет выполнена и вторая. В табл. 2.9 перечислены действия, которые необходимы для защиты информационных систем от силового деструктивного воздействия по сети питания. На практике же мы видим, что повсюду нарушаются конструкционные и структурно-функциональные требования защиты. Это и квалификация обслуживающего персонала, и дисциплина монтажа объекта, конфигурация аппаратуры, недопустимое применение комплектующих и многое другое. Приведенные методы, включая схемотехнические, должны использоваться комплексно, если нужна надежная работа аппаратуры информационнойсистемы. Иначе обязательно останется лазейка для применения технических средств силового деструктивного воздействия.

Технические средства силового деструктивного воздействия по проводным каналам

Для силового деструктивного воздействия на информационные системы по проводным линиям связи требуется существенно меньшая энергия и длительность импульсов, чем для воздействий по сетям питания. А это значит, что технические средства силового деструктивного воздействия по проводным каналам связи имеют более простую схемотехнику, обеспечивают возможность использования автономных источников питания, их габариты существенно меньше, да и стоят они дешевле, чем их сетевые аналоги. При всем этом обеспечивается высокая вероятность вывода объекта атаки из строя. Классификация технических средств силового деструктивного воздействия по проводным каналам связи приведена на рис. 2.38.

Для поражающего силового воздействия по проводным линиям связи на информационную систему необходимо, чтобы эти воздействия могли преодолеть предельную поглощающую способность компонентов, используемых во входных цепях. В этом случае, как и в случае атаки по сети питания, широко используются емкостные конденсаторные накопители. Например, средство силового воздействия с низковольтным емкостным накопителем большой энергии может быть реализовано в кейсе среднего размера и стоить 6000—8000 долларов. Необслуживаемое атакующее техническое средство с емкостной развязкой имеет размеры видеокассеты и стоит порядка 1000—1500 долларов.

В последние годы появился новый класс приборов, функционально близких к конденсаторам очень большой емкости, по существу занимающих положение между конденсаторами и источниками питания. Это — ионисторы, энергонакопительные конденсаторы с двойным электрическим слоем, заряд в которых накапливается на границе между электродом и электролитом. В качестве электрода используют высокопористые угольные материалы, благодаря чему достигается емкость порядка 10 $Ф/см^3$ и более. При большой емкости ионисторы имеют очень малые габариты. Ионистор емкостью 1 Ф на напряжение 5 В имеет объем порядка 1 $см^3$, а его удельные параметры — около 12 $Дж/см^3$.

Для вывода из строя таких электронных компонентов информационной системы, как микросхемы, транзисторы, диоды и т. п., достаточно воздействия на них импульса

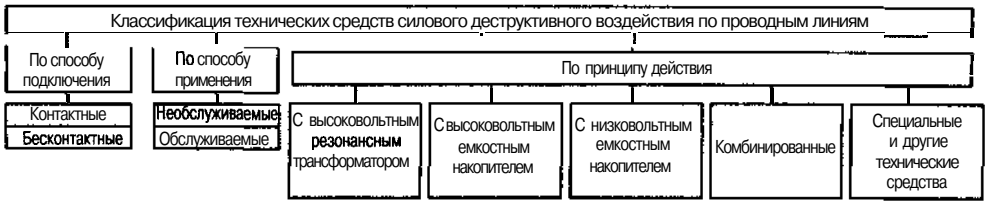


Рис. 2.38. Классификация технических средств силового деструктивного воздействия по проводным каналам связи

с энергией 1—1000 мкДж. Причем этот импульс может быть весьма коротким, так как время пробоя, например, МОП-структуры или pn-перехода составляет 10—1000 нс. Напряжение пробоя полупроводниковых переходов тоже невелико и составляет от единиц до десятков вольт. У арсенидгаллиевых приборов, например, это напряжение равно 10 В, запоминающие устройства имеют пороговые напряжения около 7 В, логические интегральные схемы на МОП-структурах — от 7 до 15 В. И даже кремниевые сильноточные биполярные транзисторы, обладающие повышенной прочностью к перегрузкам, имеют напряжение пробоя в диапазоне 15—65 В.

К классу «Специальные и другие технические средства» относятся все нетрадиционные и специфические технические средства силового деструктивного воздействия. Так, например, в составе некоторых средств деструктивного воздействия в качестве инжекторов могут быть использованы конструкционные элементы здания, канализация, водопровод, сеть питания объекта и т. п.

Для соединения отдельных компьютеров в единую информационную систему используются коаксиальные кабели или неэкранированные витые пары. Они подключаются к компьютеру через устройства гальванического разделения (трансформатор, оптопару и т. п.), которые обычно присутствуют на входе модема, сетевой платы и других узлах информационной системы.

Исходя из условий безопасности вашей аппаратуры да и вашей личной безопасности, следует посоветовать не прокладывать локальную сеть коаксиальным кабелем (где такая сеть уже работает, пусть работает, но новые рабочие места подключайте

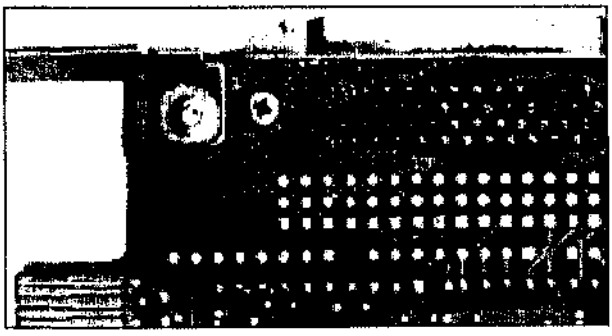


Рис. 2.39. Результат использования коаксиального кабеля

Таблица 2.10. Защита информационных систем от силового деструктивного воздействия по проводным линиям связи

Действие	Особенности
На все проводные линии связи, выходящие за пределы зоны контроля службы безопасности, установить устройства защиты от силового деструктивного воздействия	Места для установки шкафов с устройствами защиты выбираются в зонах, подконтрольных службе безопасности
Для выявления несанкционированного подключения к проводным линиям с помощью анализатора неоднородности снять контрольный «слепок» сети; систематическое сравнение текущего и контрольного «слепков» сети обеспечивает обнаружение НСД	Контрольный «слепок» снимается только после полного завершения монтажа сети проводных линий
Доступ к линиям связи, кросс-панелям, мини-АТС и другим элементам информационной системы должен быть ограничен	Ограничение обеспечивается соответствующими документами и техническими средствами
Нежелательно размещать оборудование сети (маршрутизаторов, АТС, кросса и т. п.) на внешних стенах объекта	В этом случае велика вероятность успешного проведения силового деструктивного воздействия из неконтролируемой зоны
Не применять общепринятую топологию прокладки проводных линий связи и сигнализации вдоль стены параллельно друг другу, т. к. она является идеальной для атаки на объект с помощью специальных технических средств с бесконтактным емкостным инжектором; целесообразно использовать многопарные кабели связи с витыми парами	В противном случае с помощью плоского накладного электрода и ТС СДВ оборудование может быть выведено из строя злоумышленником за 10—30 с
При закупке оборудования необходимо учитывать степень его защиты от импульсных помех; минимальная степень защищенности должна соответствовать ГОСТ Р 50746-95 при степени жесткости испытаний 3—4	Амплитуда испытательного импульса должна быть 1 кВ для 3-й степени или 2 кВ для 4-й степени испытаний
Для 1 -го рубежа необходимо установить защиту всех проводных линий от перенапряжений с помощью воздушных разрядников и варисторов; кабели связи и сигнализации следует экранировать с использованием металлорукавов, труб и коробов	Защита устанавливается как между линиями связи, так и между каждым из проводников и контуром заземления
Для защиты 2-го рубежа можно использовать комбинированные низкопороговые помехозащитные схемы из таких элементов, как газовые разрядники, варисторы, комбинированные диодные ограничители, RC- и LC-фильтры и др.	Желательно установить групповое устройство защиты, выполненное в виде шкафа с замком
Для защиты 3-го рубежа необходимо применять схемы защиты, максимально приближенные к защищаемому оборудованию	Схемы защиты 3 рубежа обычно интегрируются с разъемами, розетками, компьютерами и т. п.

витой парой). Не используйте в качестве защитного заземления батарею отопления и другие подобные предметы, так же — нулевой провод. Ведь в этом случае достаточно, пусть даже случайно, перепутать фазу и ноль, чтобы информационная сеть была выведена из строя. Результат использования коаксиального кабеля для локальной сети и неправильного использования защитного заземления представлен на рис. 2.39, и ведь это всего лишь плата, которая стояла радом с сетевой платой в сервере. Сама сетевая плата сгорела полностью.

В качестве линий связи в информационных системах широко используются неэкранированные витые пары. Поэтому рассмотрим, как же влияют на них средства силового воздействия.

Пусть техническое средство подключено к сетевому кабелю по несимметричной схеме между жилой и шиной заземления в трехпроводной сети с изолированной нейтралью и выдает высоковольтный импульс наносекундного диапазона с крутым фронтом. Если витая пара проложена совместно с сетевым кабелем в общем пластмассовом коробе (что бывает очень часто), то при разнесении их на расстояние до 100 мм и длине участка совместной прокладки более 2 миндуцированное импульсное напряжение на жилах витой пары может достигать напряжения на выходе атакующего технического средства. Энергия импульса напряжения на жилах витой пары составляет не более 50—100 мДж и слабо зависит от энергии, генерируемой техническим средством. Наибольшую опасность индуцированное импульсное напряжение может представлять для изоляции на корпус устройств гальванической развязки, которая может быть пробита, и тогда устройство развязки станет неработоспособным.

При определении уровня защиты от силового воздействия необходимо учитывать наличие на входе устройств защиты от импульсных помех. В этом случае защищаемые компоненты будут иметь существенно большую предельную энергопоглощающую способность (до 1—10 Дж для низкоскоростных устройств и до 1—10 мДж — для высокоскоростных). Однако из-за высоких цен хорошие устройства защиты пока не получили в России широкого применения. Организационные и технические мероприятия, необходимые для защиты информационных систем от силового деструктивного воздействия по проводным линиям связи, представлены в табл. 2.10.

Беспроводные технические средства силового деструктивного воздействия

Любая информационная система может быть атакована с помощью беспроводных технических средств силового деструктивного воздействия. Воздействие может осуществляться с помощью электромагнитных импульсов на такие элементы системы, как беспроводные и проводные линии связи, системы электропитания и заземления, непосредственно на электронные элементы различных блоков.

Силовое деструктивное воздействие в настоящее время является серьезным оружием против систем защиты информационных объектов. Такое оружие оправдывает свое название электромагнитной бомбы и по эффективности является более грозным для компьютерных сетей, чем программное разрушающее воздействие. В наибольшей степени это относится к мощным мобильным техническим средствам, которые могут действовать с неохраняемой территории и на значительном расстоянии. Боевое применение подобного оружия в ракетном варианте уже было зафиксировано во время войны в Персидском заливе. Применялись подобные средства и в Словакии.

Ранее задача проведения силового воздействия на радиоэлектронную аппаратуру рассматривалась в контексте действия на нее поражающих факторов ядерного взрыва (электромагнитного импульса). В настоящее время рассматривается задача не только вывода аппаратуры из строя, но и блокирования нормального ее функционирования. Новые технологии способствуют появлению эффективных средств силово-

Рис. 2.40. Классификация беспроводных технических средств силового деструктивного воздействия

го деструктивного воздействия, которые требуют большего внимания в первую очередь со стороны служб безопасности и разработчиков систем защиты. Примерная классификация технических средств силового деструктивного воздействия приведена на рис. 2.40.

Приводимые в различной литературе и других средствах информации данные говорят о больших возможностях и высокой эффективности информационного оружия, что необходимо учитывать при обеспечении защиты информации. Все рассматриваемые средства относятся к военным технологиям, однако история и реальная действительность, к сожалению, показывают, что интервалы времени между разработкой военной технологии и ее широким использованием год от года становятся все короче.

Генератор с взрывным сжатием магнитного поля — один из первых образцов электромагнитного оружия, которое было продемонстрировано еще в конце 50-х годов в лос-аламосской национальной лаборатории США. В дальнейшем в США и СССР было разработано и испытано множество модификаций такого генератора, развивавших энергию воздействия в десятки мегаджоулей, причем уровень пиковой мощности достигал десятков тераватт. На рис. 2.41 приведена упрощенная схема генератора с взрывным сжатием магнитного поля.

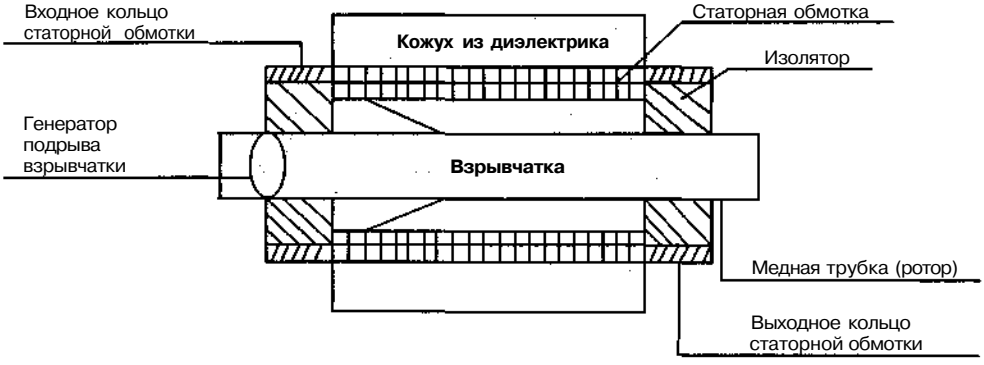


Рис. 2.41. Генератор со взрывным сжатием магнитного поля

Как видно из рис. 2.41, основа генератора с взрывным сжатием магнитного поля — цилиндрическая медная трубка с взрывчатым веществом, выполняющая функции ротора. Статором генератора служит спираль из медного провода, которая окружает роторную трубку. С помощью любого внешнего источника питания, способного обеспечить стартовый импульс электрического тока силой от нескольких килоампер, в генераторе формируется начальное магнитное поле. Подрыв взрывчатки происходит с помощью специального генератора в тот момент, когда ток в статорной обмотке достигает максимума. Образующийся при этом плоский фронт взрывной волны распространяется вдоль взрывчатки, деформируя роторную трубку и превращая ее из цилиндрической в коническую (пунктир на рисунке). В момент расширения трубки до размеров статора происходит короткое замыкание статорной обмотки, приводящее к эффекту сжатия магнитного поля и возникновению мощного импульса тока порядка нескольких десятков мегаампер.

Увеличение выходного тока по сравнению со стартовым зависит от конструкции генератора и может быть в десятки раз. В настоящее время уже удалось довести пиковую мощность генераторов с взрывным сжатием магнитного поля до десятков тераватт. Это говорит о высоких потенциальных возможностях практической реализации средств силового деструктивного воздействия.

И все же наиболее удобными в применении и наиболее перспективными в исследованиях являются высокочастотные электромагнитные средства силового воздействия, в том числе магнетроны, клистроны, гиротроны, лазеры на свободных электронах, плазменно-лучевые генераторы, а также рассмотренные выше виркаторы, которые, хотя и имеют низкий КПД (единицы процентов), но легче перестраиваются по частоте. Наиболее широкую полосу имеют плазменно-лучевые генераторы. Особенностью гиротронов является то, что они работают в миллиметровом диапазоне с высоким КПД (десятки процентов).

Рассмотрим принцип действия и конструкцию электромагнитного технического средства силового деструктивного воздействия на примере генератора с виртуальным катодом (виркатора) — рис. 2.42.

Конструкция виркатора очень проста. Опишем принцип его работы.

При подаче на анод положительного потенциала порядка 105-106 В вследствие взрывной эмиссии с катода к аноду устремляется поток электронов, который, пройдя

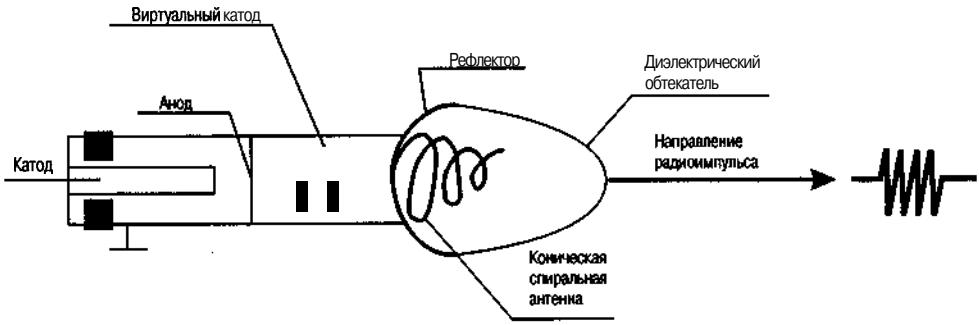


Рис. 2.42. Конструкция высокочастотного электромагнитного генератора

через сетку анода, начинает тормозиться собственным «кулоновским полем». Это поле отражает поток электронов обратно к аноду, образуя виртуальный катод. Пройдя через анод в обратном направлении, поток электронов вновь тормозится у поверхности реального катода. В результате такого взаимодействия формируется облако электронов, колеблющееся между виртуальным и реальным катодами. Образованное на частоте колебаний электронного облака СВЧ-поле антенна излучает в пространство. Токи в виркаторах, при которых возникает генерация, составляют порядка 1—10 кА. Экспериментально от виркаторов уже получены мощности от 170 кВт до 40 ГВт в сантиметровом и дециметровом диапазонах.

Существуют технические средства, использующие для излучения электромагнитных колебаний специальные антенные системы, от эффективности которых во многом зависят оперативно-технические характеристики всего комплекса силового воздействия.

При использовании новых технологий, в частности, фазированных антенных решеток, можно воздействовать сразу на несколько целей. Примером может служить система GEM2, разработанная по заказу фирмы Boeing южно-африканской фирмой PCI. Эта система состоит из 144 твердотельных излучателей импульсов длительностью менее 1 нс с суммарной мощностью 1 ГВт и ее можно устанавливать на подвижных объектах.

Несмотря на наличие направленной антенны, мощный электромагнитный импульс действует при атаке объекта на все электронные компоненты в пределах зоны электромагнитного воздействия и на все контуры, образованные связями между элементами оборудования. Выводы транзисторов, конденсаторов, микросхем и т. д. представляют собой «антенны» для электромагнитных полей высокой частоты. Ножки микросхем, например, — это набор диполей, нагруженных на сопротивления (внутреннее сопротивление интегральной схемы), причем выводы микросхемы образуют упорядоченную структуру, которая обладает свойствами антенной решетки, принимающей и усиливающей электромагнитное излучение на своей резонансной частоте. Поэтому, не являясь еще средствами селективного воздействия, широкополосные технические средства силового деструктивного воздействия наносят глобальные поражения, оправдывая установившееся название «электромагнитной бомбы» или «электромагнитной пушки».

В настоящее время многие научно-исследовательские работы заканчиваются созданием опытных образцов информационного оружия. Пример тому — американский образец оружия данного класса под условным названием MPS-II, который представляет собой генератор мощного СВЧ-излучения, использующий зеркальную антенну диаметром 3 м. Он развивает импульсную мощность около 1 ГВт (напряжение 265 кВ, ток 3,5 кА) и обладает широкими возможностями ведения информационной войны. В руководстве по применению и техническому обслуживанию определена основная его характеристика: зона поражения — 800 мот устройства в секторе 24°. Используя подобную установку, можно эффективно выводить из строя компьютерную технику, стирать записи на магнитных носителях и т. п. Поэтому актуальность проблемы защиты от электромагнитного силового воздействия сегодня, как никогда возрастает. В табл. 2.11 приведены способы и методы защиты информационных систем от беспроводных средств силового деструктивного воздействия.

Таблица 2.11. Защита информационных систем от беспроводных средств силового деструктивного воздействия

Действие	Особенности
Основным методом защиты от силового деструктивного воздействия является экранирование на всех рубежах как аппаратуры, так и помещений. При невозможности экранирования всего помещения необходимо прокладывать линии связи и сигнализации в металлических трубах или по широкой заземленной полосе металла, а также использовать специальные защитные материалы	В качестве экранирующего материала можно использовать металл, ткань, защитную краску, пленку, специальные материалы
Многорубежная защита от силового деструктивного воздействия с помощью беспроводных технических средств организуется аналогично защите по сети питания и по проводным линиям	См. табл. 2. и табл. 2.
Вместо обычных каналов связи использовать, по возможности, волоконно-оптические линии	Использование волоконно-оптических линий защищает также от возможной утечки информации
В защищенных помещениях особое внимание обратить на защиту по сети питания, используя, в первую очередь, разрядники и экранированный кабель питания	Обратить внимание, что традиционные фильтры питания от помех здесь не спасают от силового деструктивного воздействия
Учесть необходимость устранения любых паразитных излучений как защищаемой, так и вспомогательной аппаратуры	Излучения не только демаскируют аппаратуру, но и способствуют прицельному наведению электромагнитных технических средств силового деструктивного воздействия
Персоналу службы безопасности необходимо учитывать, что силовое деструктивное воздействие организуется, как правило, из неконтролируемой зоны, в то время как его деструктивное действие осуществляется по всей территории объекта	Расширение зоны контроля службы безопасности возможно за счет использования телевизионного мониторинга за пределами объекта

Основным и наиболее эффективным способом защиты от беспроводных технических средств силового деструктивного воздействия является экранирование технических средств информационных систем и помещений, в которых они находятся.

Вносимое экраном затухание зависит от материала экрана, толщины экранирующей стенки, формы экрана, характера экранируемого поля (направления распространения, поляризации и т. д.) и наличия отверстий в экране.

Расчеты, приводимые в технической литературе, показывают, что на частотах выше 100 кГц и толщине металлической стенки более 0,1 мм, независимо от формы экрана, характера поля, примененного материала (медь, сталь, алюминий), затухание полностью замкнутого экрана значительно превышает 30 дБ. То есть алюминиевая фольга толщиной 0,1 мм или несколько слоев более тонкой фольги могли бы быть прекрасным материалом для создания экранирующей конструкции, если бы удалось построить полностью замкнутый экран. На самом деле построить полностью замкнутый экран очень сложно. При построении экранирующей конструкции с затуханием 80—100 дБ начинают сказываться мельчайшие щели. По сути дела, проблема конструирования экрана сводится к проблеме исключения отверстий.

Как правило, все стыки таких экранов выполняют сварными, на разъемных стыках применяют сложные системы уплотнения, то есть создается в буквальном смысле слова герметичная конструкция. Значительные трудности возникают при размещении в экранированном пространстве воздуховодов вентиляции, а также дверных и оконных проемов.

Если оконные проемы необходимо сохранить, приходится использовать достаточно сложное сочетание металлических решеток, сеток, защитных пленок на стеклах или специальных стекол, занавесей из металлизированных тканей. Поэтому в реальном помещении получить затухание более 60 дБ — задача почти неразрешимая; обычно добиваются затухания только 20—30 дБ.

Постоянное совершенствование специальной техники стимулирует поиск новых, более эффективных электромагнитных экранов. До настоящего времени основным требованием к электромагнитным экранам всех типов являлось получение максимально возможного коэффициента затухания электромагнитной волны на выходе из материала экрана. Для этих целей могут использоваться:

- ферритодиэлектрический поглотитель электромагнитных волн;
- магнитный экран из лент аморфного металлического сплава;
- экранирующая ткань с микропроводом;
- тканый радиопоглощающий материал;
- защитная краска «Тиколак» и др.

Сверхширокополосный ферритодиэлектрический поглотитель электромагнитных волн предназначен для облицовки потолков, стен, полов помещений и представляет собой трехслойное изделие, состоящее из металлической подложки, ферритового и диэлектрического материалов, соединенных в сборную панель с помощью клея. Диэлектрический материал выполнен из пеностекла в виде клиновидных элементов. Конструктивно ферритодиэлектрический поглотитель электромагнитных волн представляет собой панель с узлами механического крепления к потолку и стенам помещения, поэтому при необходимости возможен его демонтаж без разрушения поглотителя.

Ферритодиэлектрический поглотитель электромагнитных волн является экологически чистым, при эксплуатации не выделяет вредных веществ, стабилен по своим радиотехническим характеристикам (в диапазоне от 0,03 до 40 ГГц коэффициент отражения изменяется от —12 до —40 дБ), устойчив к воздействию повышенных температур и открытого огня. Отличительной особенностью данного радиопоглощающего покрытия является оптимальное соотношение толщины и электрофизических свойств ферритового и диэлектрического материалов.

Магнитный экран из лент аморфного металлического сплава предназначен для экранирования постоянных и переменных магнитных полей радиоэлектронной аппаратуры, изготовления защитной одежды, штор, защитных занавесей в служебных помещениях, создания многослойных конструкций и объемов, экранирующих магнитное поле Земли, и т. д.. Он представляет собой гибкий листовой материал типа «рогожка» полотняного переплетения, изготовленный из лент марки КНСР шириной 850—1750 мм и толщиной 0,02—0,04 мм. Данный материал обеспечивает эффективность экранирования в 10 раз большую, чем экран из пермаллоя той же массы.

Экранирующая ткань с микропроводом предназначена для снижения уровня электромагнитного излучения в бытовых условиях не менее чем в 3 раза (от 10 дБ). Ткань

изготавливается из хлопчатобумажных нитей полотняного переплетения. В качестве активного компонента она содержит комбинированную нить, получаемую дублированием аморфного ферромагнитного микропровода в стеклянной изоляции с нитью хлопчатобумажной основы. Ткань используется для изготовления специальных штор, гардин, пошива спецодежды и т. д.

Тканый радиопоглощающий материал предназначен для поглощения энергии электромагнитного излучения. Материал главным образом применяется для защиты от СВЧ-излучения. При использовании в замкнутом пространстве материал препятствует возникновению стоячих волн. Он представляет собой гибкое тканое покрытие, которое можно крепить как непосредственно на защищаемую поверхность, так и в виде штор. Материал покрытия негорюч, прекращает горение при удалении открытого пламени, устойчив к воздействию влаги, горюче-смазочных и моющих средств, не выделяет вредных веществ. Цвет и размер материала могут быть любыми.

Защитная краска «Тиколак» позволяет получать покрытия, которые могут надежно защищать от неблагоприятного воздействия электромагнитных излучений в широком диапазоне частот от нескольких герц до десятков гигагерц. Если излучение на низких частотах в основном отражается, то на высоких частотах и СВЧ большая часть его превращается в тепло из-за возникновения вихревых токов. Меняя состав наполнителя (он является предметом ноу-хау), удается управлять соотношением отражение/поглощение. Один слой «Тиколака» толщиной всего в 70 мкм снижает интенсивность электромагнитного импульса в 3—3,5 раза.

Для получения защитного покрытия, которое во много раз снижает проникающую способность электромагнитного излучения, исходящего от внешних источников, достаточно нанести краску «Тиколак» на внутреннюю или внешнюю поверхность строения или конструкции. Краска сохраняет свои качества при температуре от —60 до +150 °С, влагостойка, не подвержена воздействию солнечных лучей. Поверх защитного покрытия «Тиколак» можно наносить любой отделочный материал: обои, краску, вагонку, керамическую плитку и т. д. Защитное покрытие ложится на гипсовые плиты для внутренних перегородок, на панели ДСП, фанеру, ДВП, стеновые панели из ПВХ, различные утеплители и т. п.

Кроме прямого воздействия электромагнитных излучений на элементы информационных систем, необходимо подавлять наводки в провода питания и иные цепи, выходящие из защищаемого помещения. С этой целью используют сетевые фильтры, но беда в том, что для достижения высокого затухания фильтр должен быть заземлен, причем заземление должно быть эффективным во всем рассматриваемом диапазоне частот.

Сеть заземления создают внутри здания для обеспечения электробезопасности, но ее же можно использовать и для усиления электромагнитной защиты кабельной проводки. Надежно защитить кабельное соединение позволяют непрерывное экранирование по всей длине кабеля и полная заделка экрана — по крайней мере, с одного конца.

Заземление сети не влияет на передачу сигнала по экранированному кабельному соединению. Электрический ток всегда «выбирает» путь с самым низким сопротивлением. Поскольку сопротивление переменному току зависит от частоты электромагнитных волн, то и «траектория» его движения определяется частотой.

Защитная сеть заземления внутри здания состоит из одиночных проводников, определенным образом соединенных. На низких частотах их сопротивление невелико и они достаточно хорошо проводят ток. При повышении частоты волновое сопротивление увеличивается и одиночный проводник начинает себя вести подобно катушке индуктивности. Соответственно переменные токи с частотой ниже 0,1 МГц будут свободно «стекать» по сети заземления, а при повышении частоты — по возможности «выбирать» альтернативный путь. Это не противоречит правилам обеспечения электробезопасности, так как сеть заземления должна гасить опасные утечки тока, исходящие от высоковольтных сетей электропитания (50—60 Гц).

Для транспортировки данных представляют интерес частоты намного выше 0,1 МГц, поэтому защитное заземление слабо влияет на передачу сигнала. В то же время любой контур заземления, выполненный проводом или даже 20—30-миллиметровой шиной, на частотах выше нескольких десятков мегагерц не только полностью перестает выполнять свои функции, но и превращается в хорошую антенну.

На высоких частотах проявляется так называемый поверхностный, или скин-эффект, который предотвращает проникновение электромагнитных полей внутрь экрана. Эффект заключается в том, что чем выше частота переменного тока через проводник, тем ближе к поверхности проводника течет этот ток. Поэтому преднамеренная или случайная электромагнитная волна отражается от внешней поверхности экрана, как луч света от зеркала. Это физическое явление не зависит от заземления, которое становится необходимым на низких частотах, когда сопротивление экрана уменьшается и токи начинают свободно распространяться по экрану и защитной сети.

Заземление экрана на одном конце провода обеспечивает дополнительную защиту сигнала от низкочастотных электрических полей, а защита от магнитных полей создается за счет сплетения проводников в витую пару. При заземлении с двух сторон образуется токовая петля, в которой случайное магнитное поле генерирует ток. Его направление таково, что создаваемое им магнитное поле нейтрализует воздействующее случайное или преднамеренное поле. Таким образом, путем двустороннего заземления осуществляется защита от воздействия случайных магнитных полей.

При использовании двустороннего заземления для случайных или преднамеренно созданных токов создается альтернативный путь по сети заземления. Если токи становятся слишком большими, кабельный экран может не справиться с ними. В этом случае для того, чтобы отвести случайные токи от экрана, необходимо обеспечить другой путь, например, параллельную шину для «земли». Решение о ее создании зависит от качества сети заземления, применяемой системы разводки питания, величины паразитных токов в сети заземления, электромагнитных характеристик среды и т. п.

На высоких частотах полное сопротивление защитной сети становится слишком большим, то есть практически исчезает электрический контакт с «землей». Чтобы предотвратить работу экрана в качестве антенны, его надо соединить с точкой, потенциал которой не изменяется, — так называемой локальной землей. Задача решается с помощью распределительного шкафа: внутри него соединяются все металлические части, и этот большой проводящий объект приобретает свойства «локальной земли».

Когда размеры проводника, например, в кабеле типа «витая пара», становятся сопоставимыми с длиной волны сигнала, проводник превращается в антенну. При увеличении частоты сигнала длина волны уменьшается и проводящий объект излучает и,

соответственно, принимает более эффективно. Излучение удается снизить за счет скручивания проводников, однако этот способ эффективен только до частоты порядка 30 МГц. Поскольку максимальная длина соединения в кабельной системе ограничена, то частоты, на которых может происходить излучение, намного выше 0,1 МГц. Это означает, что сеть заземления никак не влияет на возможное излучение экрана. Однако экран в гораздо меньшей степени является потенциальной антенной, чем кабель, по которому передается сигнал.

ГЛАВА 3. ОСНОВНЫЕ ПУТИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Наибольший интерес для злоумышленников представляют не одинокие пользователи, а корпоративные компьютерные сети. Именно в таких сетях содержится, во-первых, информация, утрата или несанкционированная модификация которой может привести к серьезным последствиям, а во-вторых, именно эта информация, как правило, интересует компьютерных взломщиков.

Защита корпоративных сетей отличается от защиты компьютеров домашних пользователей (хотя защита индивидуальных рабочих станций — неотъемлемая часть защиты сетей). И прежде всего потому, что этим вопросом занимаются грамотные специалисты по компьютерной безопасности. К тому же основа системы безопасности корпоративной сети — достижение компромисса между удобством работы для конечных пользователей и требованиями, предъявляемыми техническими специалистами.

Компьютерную систему можно рассматривать с двух точек зрения: видеть в ней лишь пользователей на рабочих станциях, а можно учитывать только функционирование сетевой операционной системы. Можно считать компьютерной сетью и совокупность проходящих по проводам пакетов с информацией. Существует несколько уровней представления сети. Точно так же можно подходить и к проблеме сетевой безопасности — на разных уровнях. Соответственно, методы защиты будут разными для каждого уровня. Чем больше уровней защищено, тем надежнее защищена и система в целом.

Первый, самый очевидный и самый трудный на практике, путь — обучение персонала поведению, затрудняющему сетевую атаку. Это вовсе не так просто, как кажется на первый взгляд. Необходимо вводить ограничения на использование Internet, причем пользователи часто не представляют, чем эти ограничения обусловлены (у них нет такой квалификации), поэтому всячески пытаются нарушать существующие запреты. Тем более, что запреты должны быть четко сформулированы. Например, совет не использовать клиентские приложения с недостаточно защищенным протоколом обычный пользователь вряд ли поймет, а вот указание не запускать на своем компьютере ICQ поймет почти наверняка.

Безопасность информации компьютерных сетей достигается проведением единой политики защитных мероприятий, а также системой мер правового, организационного и инженерно-технического характера.

При разработке необходимого уровня защиты информации в сети производится учет взаимной ответственности персонала и руководства, соблюдения интересов личности и предприятия, взаимодействия с правоохранительными органами.

Обеспечение безопасности информации достигается правовыми, организационно-административными и инженерно-техническими мерами.

Концепция защиты информации

В условиях конкурентной борьбы сохранение ведущих позиций и привлечение новых клиентов возможно только при предоставлении большего количества услуг и сокращении времени обслуживания. Это достижимо лишь при обеспечении необходимого уровня автоматизации всех операций. В то же время благодаря применению вычислительной техники не только разрешаются возникающие проблемы, но и появляются новые, нетрадиционные угрозы, связанные с искажением или физическим уничтожением информации, возможностью случайной или умышленной модификации и опасностью несанкционированного получения информации лицами, для которых она не предназначена.

Анализ существующего положения дел показывает, что уровень мероприятий, предпринимаемых для защиты информации, как правило, ниже уровня автоматизации. Такое отставание может обернуться чрезвычайно серьезными последствиями.

Уязвимость информации в автоматизированных комплексах обусловлена большой концентрацией вычислительных ресурсов, их территориальной распределенностью, долговременным хранением большого объема данных на магнитных носителях, одновременным доступом к ресурсам многих пользователей. В этих условиях необходимость принятия мер защиты, наверное, не вызывает сомнений. Однако существуют трудности:

- на сегодняшний день нет единой теории защищенных систем;
- производители средств защиты в основном предлагают отдельные компоненты для решения частных задач, оставляя вопросы формирования системы защиты и совместимости этих средств на усмотрение потребителей;
- для обеспечения надежной защиты необходимо разрешить целый комплекс технических и организационных проблем и разработать соответствующую документацию.

Для преодоления вышеперечисленных трудностей необходима координация действий всех участников информационного процесса как на отдельном предприятии, так и на государственном уровне. Обеспечение информационной безопасности — достаточно серьезная задача, поэтому необходимо, прежде всего, разработать концепцию безопасности информации, где определить национальные и корпоративные интересы, принципы обеспечения и пути поддержания безопасности информации, а также сформулировать задачи по их реализации.

Концепция — официально принятая система взглядов на проблему информационной безопасности и пути ее решения с учетом современных тенденций. Она является методологической основой политики разработки практических мер по ее реализации. На базе сформулированных в концепции целей, задач и возможных путей их решения формируются конкретные планы обеспечения информационной безопасности.

Стратегия и архитектура защиты информации

В основе комплекса мероприятий по информационной безопасности должна быть стратегия защиты информации. В ней определяются цели, критерии, принципы и процедуры, необходимые для построения надежной системы защиты. В хорошо разработанной стратегии должны найти отражение не только степень защиты, поиск брешей, места установки брандмауэров или proxy-серверов и т. п. В ней необходимо еще четко определить процедуры и способы их применения для того, чтобы гарантировать надежную защит.

Важнейшей особенностью общей стратегии информационной защиты является исследование системы безопасности. Можно выделить два основных направления:

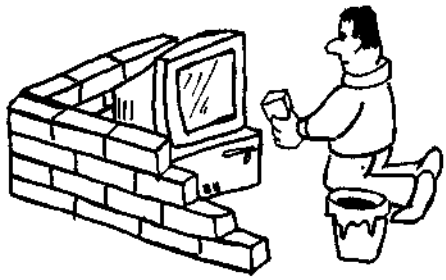
- анализ средств защиты;
- определение факта вторжения.

На основе концепции безопасности информации разрабатываются стратегия безопасности информации и архитектура системы защиты информации (рис. 3.1). Следующий этап обобщенного подхода к обеспечению безопасности состоит в определении политики, содержание которой — наиболее рациональные средства и ресурсы, подходы и цели рассматриваемой задачи.

Разработку концепции защиты рекомендуется проводить в три этапа (рис. 3.2). На первом этапе должна быть четко определена целевая установка защиты, т. е. какие реальные ценности, производственные процессы, программы, массивы данных необходимо защищать. На этом этапе целесообразно дифференцировать по значимости отдельные объекты, требующие защиты.

На втором этапе должен быть проведен анализ преступных действий, которые потенциально могут быть совершены в отношении защищаемого объекта. Важно определить степень реальной опасности таких наиболее широко распространенных преступлений, как экономический шпионаж, терроризм, саботаж, кражи со взломом. Затем нужно проанализировать наиболее вероятные действия злоумышленников в отношении основных объектов, нуждающихся в защите.

Рис. **3.1.** Иерархический подход к обеспечению безопасности информации



Главной задачей третьего этапа является анализ обстановки, в том числе местных специфических условий, производственных процессов, уже установленных технических средств защиты.

Концепция защиты должна содержать перечень организационных, технических и других мер, которые обеспечивают максимальную безопасность при заданном остаточном риске и минимальные затраты на их реализацию.

Политика защиты — это общий документ, где перечисляются правила доступа, определяются пути реализации политики и описывается базовая архитектура среды защиты.

Сам по себе документ состоит из нескольких страниц текста. Он формирует основу физической архитектуры сети, а содержащаяся в нем информация определяет выбор продуктов защиты. При этом документ может и не включать списка необходимых закупок, но выбор конкретных компонентов после его составления должен быть очевидным.

Политика защиты выходит далеко за рамки простой идеи «не впускать злоумышленников». Это очень сложный документ, определяющий доступ к данным, характер серфинга в WWW, использование паролей или шифрования, отношение к вложениям в электронную почту, использование Java и ActiveX и многое другое. Он детализирует эти правила для отдельных лиц или групп. Нельзя забывать и об элементарной физической защите. Ведь если кто-нибудь может войти в серверную комнату и получить доступ к основному файловому серверу или выйти из офиса с резервными дискетами и дисками в кармане, то все остальные меры становятся попросту бессмысленными.

Конечно, политика не должна позволять чужакам проникнуть в сеть, но, кроме того, она должна устанавливать контроль и над потенциально нечистоплотными сотрудниками вашей организации. Девиз любого администратора системы защиты — «Никому не доверяй!».

На первом этапе разработки политики прежде всего необходимо определиться, каким пользователям какая информация и какие сервисы доступны, какова вероятность нанесения вреда и какая защита уже есть.

Кроме того, политика защиты должна диктовать иерархию прав доступа, т. е. пользователям следует предоставить доступ только к той информации, которая действительно нужна им для выполнения своей работы.

Политика защиты должна обязательно отражать следующее:

- контроль доступа (запрет на доступ пользователя к материалам, которыми ему не разрешено пользоваться);

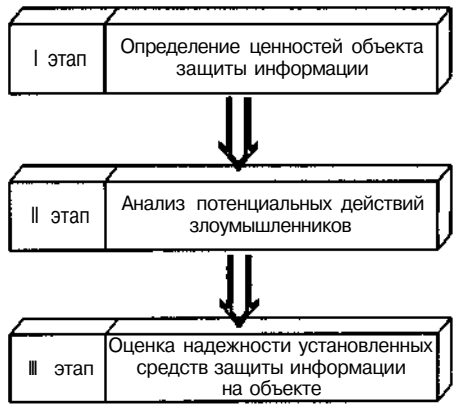


Рис. **3.2.** Этапы разработки концепции защиты информации

- ❑ идентификацию и аутентификацию (использование паролей или других механизмов для проверки статуса пользователя);
- G учет (запись всех действий пользователя в сети);
- ❑ контрольный журнал (журнал позволяет определить, когда и где произошло нарушение защиты);
- ❑ аккуратность (защита от любых случайных нарушений);
- ❑ надежность (предотвращение монополизации ресурсов системы одним пользователем);
- ❑ обмен данными (защита всех коммуникаций).

Доступ определяется политикой в отношении брандмауэров: доступ к системным ресурсам и данным из сети можно описать на уровне операционной системы и при необходимости дополнить программами защиты независимых разработчиков.

Пароли могут быть самой ценной частью вашей среды защиты, но при неправильном использовании или обращении они могут стать ключом в вашу сеть. Политика правильного использования паролей особенно полезна при управлении временными бюджетами, чтобы кто-нибудь не воспользовался действительным паролем после того, как временные сотрудники или подрядчики завершили работу.

Некоторые операционные системы предлагают также такую возможность, как квалификация, т. е. вводят минимальный уровень трудности паролей. В этих системах администратор защиты может просто задать правило «Не использовать легко угадываемых паролей». Например, пароль, в котором указаны только имя и возраст пользователя, система не примет. Конечные же пользователи обычно выбирают самые простые пути. Если им приходится иметь дело со слишком большим числом паролей, они будут использовать один и тот же пароль или задавать легко запоминаемые пароли, или, хуже того, записывать их на листке и хранить в ящике стола.

Изобилие устройств защиты, брандмауэров, шлюзов и VPN (виртуальная частная сеть), а также растущий спрос на доступ к корпоративным данным со стороны сотрудников, партнеров и заказчиков, ведет к созданию сложной среды защиты, трудной для управления. Правила для многих из перечисленных устройств приходится часто задавать отдельно.

По мере того как крупные корпорации продолжают объединяться и поглощать более мелкие компании, среда защиты (и сеть в целом) все чаще принимает бессистемный характер. Когда это происходит, управлять правилами становится чрезвычайно трудно.

Брандмауэры (как аппаратные, так и программные) позволяют определить, кто имеет право доступа в вашу сеть извне. Все брандмауэры реализуют те или иные правила; разница состоит в уровне детализации и простоте использования, обеспечиваемой интерфейсом управления.

В идеале брандмауэр позволяет решить три задачи:

- ❑ задавать правила из интуитивно понятного графического интерфейса;
- ❑ управлять доступом вплоть до уровня индивидуальных файлов и объектов;
- О группировать файлы и объекты для коллективного применения к ним правил в целях упрощения управления.

На сетевом уровне управлять защитой с помощью правил можно несколькими способами. Один из распространенных способов — с помощью адресации, когда пользователи приписываются к конкретной внутренней подсети для ограничения уровня их дос-

тупа. Фильтрация пакетов позволяет пропускать или блокировать пакеты в момент пересечения ими некоторых границ в зависимости от адреса отправителя или получателя.

Системы защиты функционируют на прикладном уровне; в этом случае системы или приложения, которым адресованы пакеты, запрашивают у пользователя пароль, проверяют его и затем предоставляют доступ в соответствии с предопределенными правилами.

Виртуальная частная сеть (VPN) по своей природе уже определяется некоторыми правилами (во всяком случае, так должно быть). VPN — это защищенный канал между несколькими офисами через общедоступную сеть, который представляет собой экономически выгодный способ связать друг с другом многочисленные филиалы, партнеров и заказчиков.

В простейшем случае сеть VPN связывает двух или более лиц или групп по защищенному соединению. В идеале организация этого соединения определяется совокупностью правил. Однако данная простейшая модель не учитывает необходимости контроля доступа: к чему будет иметь доступ удаленный пользователь после подключения к сети VPN?

Конечная цель сети VPN — введение строгих детализированных правил: с увеличением размеров сеть VPN требует более жесткого надзора, определения правил и их соблюдения.

Некоторые сети VPN предназначены не для замены брандмауэров, у которых есть свои правила, а, скорее, для их дополнения. В идеале правила для обеих систем должны быть согласованы. Правила VPN регламентируют в первую очередь, как пользователи могут подключиться к сети: уровень шифрования, использование паролей и другие зависящие от соединения факторы. Ничто не угрожает защите больше, чем активный код. Благодаря ActiveX и Java компьютерные программы получили возможность перемещаться по WWW, позволяя тем самым проделывать всевозможные полезные трюки, а также открывая возможность проводить опасные атаки на сеть.

Помимо введения ограничений на тип активного кода, политика защиты в отношении WWW может запрещать доступ из корпоративной сети к определенным IP-адресам. Часто причиной введения подобных ограничений являются не столько требования защиты, сколько политика в отношении персонала.

Тем не менее иногда запрещение доступа к определенным узлам бывает обусловлено соображениями защиты, в первую очередь это касается хакерских серверов, откуда сотрудник может непреднамеренно загрузить вредоносный апплет или почерпнуть информацию, которую он может использовать для атаки на сеть. Нужно постоянно помнить, что большинство атак совершается сотрудниками организации, так что предусмотрительность не помешает.

Политика защиты — это всего лишь бумажный документ. Для ее реализации и соблюдения требуется технология. Более того, как только политика будет разработана, ее предстоит воплотить в жизнь.

Один из простейших способов реализовать защиту — поручить заняться этим специализированной компании. К тому же, одна из самых грубых ошибок, совершаемых многими, состоит в том, что, разработав политику и купив оборудование, они на том и успокаиваются.

Систему защиты сначала надо правильно подключить, а потом ее необходимо регулярно пересматривать. Потребности, задачи и правила могут со временем измениться.

Если система не будет постоянно адаптироваться с учетом этих изменений, то в ней неизбежно появятся «дыры».

Большинство предложений сторонних услуг предусматривает предоставление заказчику интерфейса на базе WWW, откуда он может брать изменения. Несмотря на удобство, такой подход не обеспечивает всех необходимых средств контроля.

Важной частью создания политики защиты является планирование. Установив свои потребности до начала реализации и проанализировав их вплоть до уровня всех подразделений, вы сможете в результате создать гораздо лучший проект организации защиты, особенно в долгосрочной перспективе.

Определение политики ничего не дает, если она не соблюдается, впрочем, как ничего не дает и установка устройств защиты, если их оставляют без присмотра.

Защита — сложный и часто противоречивый процесс, реализация и управление которым осуществляется с помощью множества подчас слабо связанных между собой устройств и программ.

Политика безопасности информации

При разработке политики безопасности информации, в общем случае, первоначально определяют объекты, которые надо защитить, и их функции. Затем оценивают степень интереса потенциального противника к этим объектам, вероятные виды нападения и вызываемый ими ущерб. Наконец, определяют уязвимые для воздействия области, в которых имеющиеся средства противодействия не обеспечивают достаточной защиты.

Для эффективной защиты нужно оценить каждый объект с точки зрения возможных угроз и видов нападения, потенциальной вероятности применения специальных инструментов, оружия и взрывчатых веществ. Особо важным допущением в этом процессе является предположение о том, что наиболее ценный для потенциального злоумышленника объект привлечет пристальное внимание злоумышленника и будет служить вероятной целью, против которой он использует основные силы. При этом разработка политики безопасности информации должна проводиться с учетом задач, решение которых обеспечит реальную защиту данного объекта (рис. 3.3).

Средства противодействия должны соответствовать концепции полной и эшелонированной защиты. Это означает, что их следует размещать на концентрических кругах, в центре которых находится объект защиты. В этом случае все возможные пути противника к любому объекту будут пересекать эшелонированную систему защиты. Каждый рубеж обороны организуется так, чтобы задержать нападающего на время, достаточное для принятия персоналом охраны ответных мер.

На заключительном этапе выбранные средства противодействия объединяют в соответствии с принятой концепцией защиты. Производится предварительная оценка начальной и ожидаемой общей стоимости жизненного цикла всей системы. В частности, следует учитывать возможные перемещения объектов, а также изменение требований в местах входа.

В том случае, когда внутри одного здания расположены объекты, требования к защите которых существенно различаются, здание делят на отсеки. Таким образом выделяют внутренние периметры внутри общего контролируемого пространства и создают внутренние защитные средства от несанкционированного доступа. Периметр обычно определяется физическими препятствиями, проход через которые контролируется электронным способом или с помощью специальных процедур, выполняемых сотрудниками охраны.

При защите группы зданий, имеющих общую границу или периметр, необходимо учитывать не только отдельный объект или здание, но и место их расположения. Обычно участки местности с большим количеством зданий имеют общие или частично совпадающие требования по обеспечению безопасности, а некоторые участки имеют ограждение по периметру и единую проходную. Организовав общий периметр, можно уменьшить количество защитных средств в каждом здании и установить их только для важных объектов, нападение на которые наиболее вероятно. Аналогичным образом, каждое строение или объект на участке оценивают с точки зрения их возможностей задержать нападающего.

Анализируя перечисленные требования, видим, что все они сводятся к исключению возможности неправомочного доступа к устройствам обработки и передачи информации, похищения носителей информации и саботажа.

Систему безопасности зданий и помещений и самих информационных средств целесообразно организовать в виде концентрических колец (стратегическое сердце в центре), размещая пункты контроля на переходах от одной зоны к другой (рис. 3.4). Что же касается контроля доступа в здания и помещения информационной службы, то основная мера — разделение и изоляция не только зданий и помещений, но и комплексов средств по их функциональному предназначению. Применяется как автоматическая, так и неавтоматическая система контроля доступа в здания и помещения. Система контроля может быть дополнена средствами наблюдения в дневное и ночное время (контроль за всеми входами без мертвых зон).

Выбор физических средств безопасности основывается на предварительном изучении важности объекта защиты, расходов на них и степени надежности системы конт-

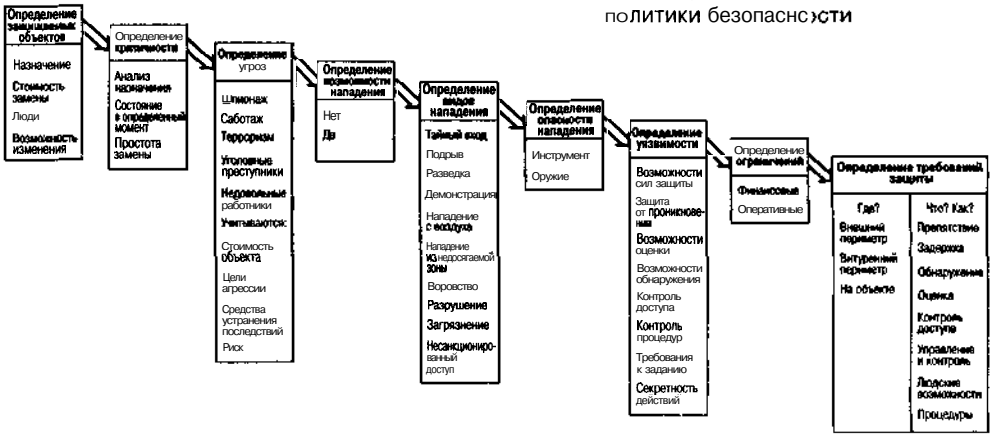


Рис. 3.3. Комплекс учета задач при разработке политики безопасности

Зона 1. Внешняя зона безопасности КС.
Обеспечение:- физические препятствия (ограждение)
- проходные по периметру
- неавтоматическая система контроля допуска на территорию

Зона 2. Средняя зона безопасности КС.
Обеспечение:- пункты контроля с электронной защитой дверей
- видеонаблюдение
- исключение мертвых зон

Зона 3. Внутренняя зона безопасности КС
Обеспечение:- доступ к ПК сети только через контрольную систему
-биометрические системы идентификации

Рис. 3.4. Система безопасности компьютерной сети в здании

роля доступа (стоимость ненадежного предупреждения при реальном праве и стоимость надежного предупреждения при ложном праве), социальных аспектов и человеческих слабостей. В случае реализации кольцевой системы контроля доступа с высокой степенью безопасности возможно использование биометрической идентификации: отпечатков пальцев, ладоней, кровеносных сосудов сетчатки глаза или распознавание речи. Предусмотрен специальный режим допуска персонала, обслуживающего технические средства на договорной основе. Эти лица после идентификации допускаются на объект с сопровождающим лицом. Кроме того, для них точно устанавливается режим посещения, пространственные ограничения, время прибытия и убытия, характер выполняемой работы.

Наконец, по периметру здания устанавливают комплексное наблюдение с помощью системы различных датчиков определения вторжения. Эти датчики связаны с центральным постом охраны объекта и контролируют все возможные точки вторжения, особенно в нерабочее время.

Периодически следует проверять надежность физической защиты дверей, окон, крыши, вентиляционных отверстий и других выходов. В частности, проверяют сопротивляемость дверей против взлома (наличие и надежность заграждения, замков и пр.) и окон (доступность с внешней стороны, прочность рам, решеток). Наконец, убеждаются в защищенности воздухозаборников (решетки или выходов кондиционеров, вентиляторов и т. д.), особенно с учетом возможности реализации злонамеренных угроз.

Каждое помещение определяется как зона, которая имеет свою систему доступа в зависимости от важности находящегося в ней содержимого. Система допуска должна быть селективной, ранжированной по уровням в зависимости от важности лица или объекта. Система допуска может быть централизованной (управление разрешениями, планирование расписаний и календарных планов, письменные образцы допусков прибывающих и убывающих и т. д.). Контролировать доступ можно с помощью значков или жетонов.

Степень такого доступа может быть самой различной: от ложного права до полного доступа. Выбирают защиту в зависимости от возможностей ее организации. Можно организовать, например, визуальное наблюдение с помощью телевизионного контроля, подкрепленное с целью точного контроля временным графиком персонального доступа прибытия и убытия исполнителей. Самый жесткий контроль доступа в залы, где находится особо важная стратегическая информация, обеспечивается

биометрическими методами. Можно создать дополнительную систему предупреждения вторжения в залы (в частности, в нерабочее время для залов без обслуживающего персонала).

Системы контроля нужно периодически проверять и постоянно поддерживать в рабочем состоянии. Для этого существуют специализированные подразделения и органы контроля.

Наконец, должно быть налажено информирование руководства и обучение персонала по различным вопросам предупреждения и контроля доступа на основе анализа результатов работы системы безопасности предприятия.

Обязательно нужно проверять систему доступа во вспомогательные помещения (помещение охраны, архивы, рабочие места анализа и программирования), в частности, наличие и адекватность системы контроля установленным требованиям.

Можно также предусмотреть различные способы защиты малогабаритного оборудования, таких как персональные компьютеры и средства физической защиты (ставни или надежные запоры, футляры для хранения, дополнительные платы логических запирающих устройств, кнопки включения сигнала тревоги под средствами обработки информации).

Подводя итоги вышесказанному, рассмотрим, как определяется политика безопасности информации при защите компьютерных сетей. Обычно для корпоративных сетей с большим количеством пользователей составляется специальный документ, регламентирующий работу в сети, называемый «Политика безопасности».

Политика обычно состоит из двух частей: общих принципов и конкретных правил работы. Общие принципы определяют подход к безопасности в Internet. Правила же регламентируют, что разрешено, а что запрещено. Правила могут дополняться конкретными процедурами и различными руководствами.

Правда, существует и третий тип политики; его описание встречается в литературе по безопасности в Internet — технический подход-анализ, который помогает выполнять принципы и правила политики. Однако он слишком техничен и сложен для понимания руководством организации, поэтому не так широко используется, как политика. Тем не менее он обязателен при описании возможных решений, определяющих компромиссы политики.

Обычно политика безопасности регламентирует использование основных сервисов сети (электронную почту, WWW и т. п.), а также ставит в известность пользователей сети о тех правах доступа, какими они обладают, что обычно определяет и процедуру аутентификации пользователя.

К этому документу следует относиться со всей серьезностью. Все остальные стратегии защиты строятся на предположении, что правила политики безопасности неукоснительно соблюдаются. Политика безопасности вызывает и большинство нареканий со стороны пользователей, потому что в ней очевидным образом написано, что именно пользователю воспрещено. Рядовому пользователю может быть непонятен запрет, скажем, на использование служебного адреса электронной почты для личной переписки. Однако политика безопасности — это официальный документ, который составляется на основе, с одной стороны, производственной необходимости в сервисах, предоставляемых Internet, а с другой — на основе требований безопасности, сформулированных соответствующими специалистами-профессионалами.

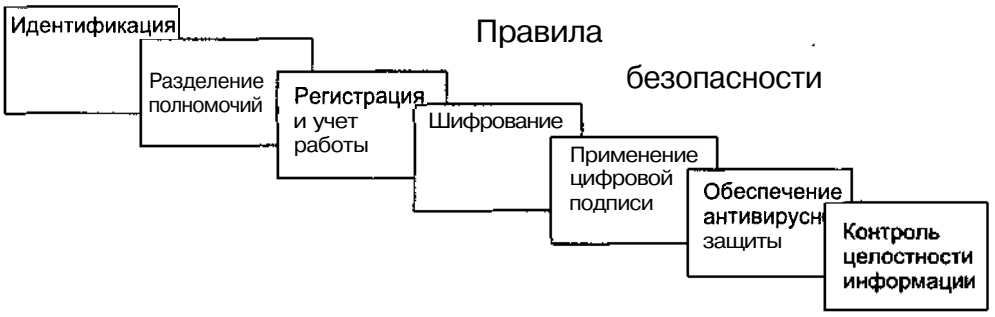


Рис. 3.5. Основные правила обеспечения политики безопасности информации

Автоматизированный комплекс можно считать защищенным, если все операции выполняются в соответствии со строго определенными правилами (рис. 3.5), которые обеспечивают непосредственную защиту объектов, ресурсов и операций. Основу для формирования требований к защите составляет список угроз. Когда такие требования известны, могут быть определены соответствующие правила обеспечения защиты. Эти правила, в свою очередь, определяют необходимые функции и средства защиты. Чем строже требования к защите и больше соответствующих правил, тем эффективнее ее механизмы и тем более защищенным оказывается автоматизированный комплекс.

Из вышеизложенного следует, что защита информации в компьютерной сети эффективнее в том случае, когда проектирование и реализация системы защиты происходит в три этапа:

- анализ риска;
- реализация политики безопасности;
- поддержка политики безопасности.

На первом этапе анализируются уязвимые элементы компьютерной сети, определяются и оцениваются угрозы и подбираются оптимальные средства защиты. Анализ риска заканчивается принятием политики безопасности. Политикой безопасности (Security Policy) называется комплекс взаимосвязанных мер, направленных на обеспечение высокого уровня безопасности. В теории защиты информации считается, что эти меры должны быть направлены на достижение следующего:

- конфиденциальность (засекреченная информация должна быть доступна только тому, кому она предназначена);
- целостность (информация, на основе которой принимаются решения, должна быть достоверной и полной, а также защищена от возможных непреднамеренных и злоумышленных искажений);
- готовность (информация и соответствующие автоматизированные службы должны быть доступны и в случае необходимости готовы к обслуживанию).

Уязвимость означает невыполнение хотя бы одного из этих свойств.

Для компьютерных сетей можно выделить следующие вероятные угрозы, которые необходимо учитывать при определении политики безопасности:

- несанкционированный доступ посторонних лиц, не принадлежащих к числу служащих, и ознакомление с хранимой конфиденциальной информацией;

- ознакомление своих служащих с информацией, к которой они не должны иметь доступа;
- несанкционированное копирование программ и данных;
- перехват и ознакомление с конфиденциальной информацией, передаваемой по каналам связи;
- кража магнитных носителей, содержащих конфиденциальную информацию;
- кража распечатанных документов;
- случайное или умышленное уничтожение информации;
- несанкционированная модификация служащими документов и баз данных;
- фальсификация сообщений, передаваемых по каналам связи;
- отказ от авторства сообщения, переданного по каналам связи;
- отказ от факта получения информации;
- навязывание ранее переданного сообщения;
- ошибки в работе обслуживающего персонала;
- разрушение файловой структуры из-за некорректной работы программ или аппаратных средств;
- разрушение информации, вызванное вирусными воздействиями;
- разрушение архивной информации, хранящейся на магнитных носителях;
- кража оборудования;
- ошибки в программном обеспечении;
- отключение электропитания;
- сбои оборудования.

Оценка вероятности появления данных угроз и ожидаемых размеров потерь — трудная задача. Еще сложнее определить требования к системе защиты. Политика безопасности должна определяться следующими мерами:

- идентификация, проверка подлинности и контроль доступа пользователей на объект, в помещения, к ресурсам автоматизированного комплекса;
- разделение полномочий пользователей, имеющих доступ к вычислительным ресурсам;
- регистрация и учет работы пользователей;
- регистрация попыток нарушения полномочий;
- шифрование конфиденциальной информации на основе криптографических алгоритмов высокой стойкости;
- применение цифровой подписи для передачи информации по каналам связи;
- обеспечение антивирусной защиты (в том числе и для борьбы с неизвестными вирусами) и восстановление информации, разрушенной вирусными воздействиями;
- контроль целостности программных средств и обрабатываемой информации;
- восстановление разрушенной архивной информации, даже при значительных потерях;
- наличие администратора (службы) защиты информации в системе;
- выработка и соблюдение необходимых организационных мер;
- применение технических средств, обеспечивающих бесперебойную работу оборудования.

Второй этап — реализация политики безопасности — начинается с проведения расчета финансовых затрат и выбора соответствующих средств для выполнения этих

задач. При этом необходимо учесть такие факторы как бесконфликтность работы выбранных средств, репутация поставщиков средств защиты, возможность получения полной информации о механизмах защиты и предоставляемые гарантии. Кроме того, следует учитывать принципы, в которых отражены основные положения по безопасности информации:

- экономическая эффективность (стоимость средств защиты должна быть меньше, чем размеры возможного ущерба);
- минимум привилегий (каждый пользователь должен иметь минимальный набор привилегий, необходимый для работы);
- простота (защита будет тем более эффективной, чем легче пользователю с ней работать);
- отключение защиты (при нормальном функционировании защита не должна отключаться, за исключением особых случаев, когда сотрудник со специальными полномочиями может иметь возможность отключить систему защиты);
- открытость проектирования и функционирования механизмов защиты (секретность проектирования и функционирования средств безопасности — не лучший подход к защите информации, т. к. специалисты, имеющие отношение к системе защиты, должны полностью представлять себе принципы ее функционирования и в случае возникновения затруднительных ситуаций адекватно на них реагировать);
- независимость системы защиты от субъектов защиты (лица, занимавшиеся разработкой системы защиты, не должны быть в числе тех, кого эта система будет контролировать);
- всеобщий контроль (любые исключения из множества контролируемых субъектов и объектов защиты снижают защищенность автоматизированного комплекса);
- отчетность и подконтрольность (система защиты должна предоставлять достаточно доказательств, показывающих корректность ее работы);
- ответственность (личная ответственность лиц, занимающихся обеспечением безопасности информации);
- изоляция и разделение (объекты защиты целесообразно разделять на группы таким образом, чтобы нарушение защиты в одной из групп не влияло на безопасность других групп);
- отказ по умолчанию (если произошел сбой средств защиты и разработчики не предусмотрели такой ситуации, то доступ к вычислительным ресурсам должен быть запрещен);
- полнота и согласованность (система защиты должна быть полностью специфицирована, протестирована и согласована);
- параметризация (защита становится более эффективной и гибкой, если она допускает изменение своих параметров со стороны администратора);
- принцип враждебного окружения (система защиты должна проектироваться в расчете на враждебное окружение и предполагать, что пользователи имеют наихудшие намерения, что они будут совершать серьезные ошибки и искать пути обхода механизмов защиты);
- привлечение человека (наиболее важные и критические решения должны приниматься человеком, т. к. компьютерная система не может предусмотреть все возможные ситуации);

- отсутствие излишней информации о существовании механизмов защиты (существование механизмов защиты должно быть по возможности скрыто от пользователей, работа которых контролируется).

Поддержка политики безопасности — третий, наиболее важный, этап. Мероприятия, проводимые на данном этапе, требуют постоянного наблюдения за происходящими вторжениями в сеть злоумышленников, выявления «дыр» в системе защиты объекта информации, учета случаев несанкционированного доступа к конфиденциальным данным.

При этом основная ответственность за поддержание политики безопасности сети лежит на системном администраторе, который должен оперативно реагировать на все случаи взлома конкретной системы защиты, анализировать их и использовать необходимые аппаратные и программные средства защиты с учетом максимальной экономии финансовых средств.

Требования к безопасности компьютерных сетей в РФ

Руководящие документы, относящиеся к области защиты информации для компьютерных сетей, разработаны Государственной технической комиссией при Президенте Российской Федерации. Требования всех этих документов обязательны для исполнения только в государственном секторе, либо коммерческими организациями, которые обрабатывают информацию, содержащую государственную тайну. Для остальных коммерческих структур документы носят рекомендательный характер.

Рассмотрим содержание одного из документов, отражающих требования по защите информации от несанкционированного доступа. Полное название документа — «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации».

В этом документе приведена классификация автоматизированных систем на классы по условиям их функционирования с точки зрения защиты информации в целях разработки и применения обоснованных мер по достижению требуемого уровня безопасности.

Устанавливается девять классов защищенности (табл. 3.1), каждый из которых характеризуется определенной минимальной совокупностью требований по защите.

Классы подразделяются на три группы, отличающиеся особенностями обработки информации. В пределах каждой группы соблюдается иерархия требований по защите в зависимости от ценности (конфиденциальности) информации и, следовательно, иерархия классов защищенности. Рассмотрим показатели каждой из групп, начиная с последней.

Третья группа включает системы, в которых работает один пользователь, допущенный ко всей информации, размещенной на носителях одного уровня конфиденциальности. Группа содержит два класса — 3Б и 3А.

Таблица 3.1. Классы защищенности компьютерных сетей

Требования	Классы								
	3Б	3А	2Б	2А	1Д	1Г	1В	1Б	1А
К подсистеме управления доступом									
Идентификация, проверка подлинности и контроль доступа субъектов:									
- к системе	X	X	X	X	X	X	X	X	X
- к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ	—	—	—	X	—	X	X	X	X
- к программам	—	—	—	X	—	X	X	X	X
- к томам, каталогам, файлам, записям	—	—	—	X	—	X	X	X	X
Управление потоками информации	—	—	—	X	—	—	X	X	X
К подсистеме регистрации и учета									
Регистрация и учет:									
- входа (выхода) субъектов в(из) системы (узла сети)	X	X	X	X	X	X	X	X	X
- выдачи печатных (графических) выходных документов	—	X	—	X	—	X	X	X	X
- запуска (завершения) программы и процессов (заданий, задач)	—	X	—	X	—	X	X	X	X
- доступа программ субъектов доступа к защищаемым файлам, включая их создание и удаление, передачу по линиям и каналам связи	—	—	—	X	—	X	X	X	X
- доступа программ субъектов доступа к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программным томам, каталогам, файлам, записям, полям записей	—	—	—	X	—	X	X	X	X
- изменения полномочий субъектов доступа	—	—	—	—	—	—	X	X	X
- создаваемых защищаемых объектов доступа	—	—	—	X	—	—	X	X	X
Учет носителей информации	X	X	X	X	X	X	X	X	X
Очистка (обнуление, обезличивание) оперативной памяти и внешних накопителей	—	X	—	X	—	X	X	X	X
Сигнализация попыток нарушения защиты	—	—	—	—	—	X	X	X	X
К криптографической подсистеме									
Шифрование конфиденциальной информации	—	—	—	—	—	—	X	X	X
Шифрование информации, принадлежащей различным субъектам доступа (группам субъектов) на разных ключах	—	—	—	—	—	—	—	—	X
Использование аттестованных (сертифицированных) криптографических средств	—	—	—	—	—	—	—	X	X

Продолжение табл. 3.1

К подсистеме обеспечения целостности									
Обеспечение целостности программных средств и обрабатываемой информации	X	X	X	X	X	X	X	X	X
Физическая охрана средств вычислительной техники и носителей информации	X	X	X	X	X	X	X	X	X
Наличие администратора (службы) защиты информации	—	—	—	X	—	—	X	X	X
Периодическое тестирование СЗИ	X	X	X	X	X	X	X	X	X
Наличие средств восстановления СЗИ	X	X	X	X	X	X	X	X	X
Использование сертифицированных средств защиты	—	X	—	X	—	—	X	X	X

Вторая группа включает системы, в которых пользователи имеют одинаковые права доступа ко всей информации, обрабатываемой и/или хранимой на носителях различного уровня конфиденциальности. Группа содержит два класса — 2Б и 2А.

Первая группа включает многопользовательские системы, в которых одновременно обрабатывается и/или хранится информация разных уровней конфиденциальности. Группа содержит пять классов — 1Д, 1Г, 1В, 1Б и 1А.

В общем плане защитные мероприятия охватывают 4 подсистемы:

- управления доступом;
- регистрации и учета;
- криптографической;
- обеспечения целостности.

Показатели защищенности средств вычислительной техники от НСД приведены в документе «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности». В нем определены 7 классов защищенности этих средств от НСД к информации. Самый низкий класс — седьмой, самый высокий — первый. Каждый класс наследует требования защищенности от предыдущего.

Изложенные ниже требования к показателям защищенности предъявляются к общесистемным программным средствам и операционным системам. Все средства защиты вычислительной техники представляют собой единый комплекс. В зависимости от реализованных моделей защиты и надежности их проверки классы подразделяются на 4 группы.

Первая группа включает только седьмой класс (минимальная защищенность).

Вторая группа характеризуется избирательной защитой и включает шестой и пятый классы. Избирательная защита предусматривает контроль доступа поименованных субъектов к поименованным объектам системы. При этом для каждой пары «субъект-объект» должны быть определены разрешенные типы доступа. Контроль доступа применяется к каждому объекту и каждому субъекту (индивиду или группе равноправных индивидов).

Третья группа характеризуется полномочной защитой и включает четвертый, третий и второй классы. Полномочная защита предусматривает присвоение каждому субъекту и объекту системы классификационных меток, указывающих его место в со-

ответствующей иерархии. Классификационные метки на объекты устанавливаются пользователем системы или специально выделенным субъектом. Обязательным требованием для классов, входящих в эту группу, является реализация диспетчера доступа (reference monitor — монитор ссылок). Контроль доступа должен осуществляться применительно ко всем объектам при явном и скрытом доступе со стороны любого из субъектов. Решение о санкционировании запроса на доступ должно приниматься только при одновременном разрешении его и избирательными, и полномочными правилами разграничения доступа.

Четвертая группа характеризуется верифицированной защитой и содержит только первый класс.

Для присвоения класса защищенности система должна иметь:

- руководство администратора по системе;
- руководство пользователя;
- тестовую и конструкторскую документацию.

В качестве примера рассмотрим требования к подсистеме обеспечения целостности класса 2А.

Подсистема обеспечения целостности класса 2А должна обеспечивать целостность программных средств системы защиты информации от несанкционированного доступа, целостность обрабатываемой информации, а также неизменность программной среды. При этом:

- G целесообразность проверяется при загрузке системы по наличию имен (идентификаторов) компонентов системы защиты информации;
- О целостность программной среды обеспечивается отсутствием в системе средств разработки и отладки программ,
- физическая охрана средств (устройств и носителей информации) предусматривает постоянную охрану территории и здания, где размещается система, с помощью технических средств и специального персонала, использование строгого пропускного режима, специальное оборудование помещений;
- должен быть администратор (служба) защиты информации, ответственный за ведение, нормальное функционирование и контроль работы системы защиты информации от НСД;
- необходимо периодическое тестирование функций системы защиты информации от НСД при изменении программной среды и персонала системы с помощью тест-программ, имитирующих попытки НСД;
- должны быть в наличии средства восстановления защиты, предусматривающие ведение двух копий программных средств защиты, их периодическое обновление и контроль работоспособности;
- следует использовать сертифицированные средства защиты.

Тщательный анализ таких требований позволит оценить реальную безопасность любой информационной системы с отнесением ее к определенному классу защищенности.

Виды обеспечения безопасности информации

Совсем недавно к интеллектуальным преступлениям можно было бы отнести незаконное копирование произведений и товарных знаков, присвоение авторства и т. п. В настоящее время в связи с широким распространением вычислительной техники и средств телекоммуникаций список таких преступлений значительно расширился. Они происходят теперь и в экономической сфере. А это высокорентабельный бизнес, который не считается ни со временем, ни с расстояниями, ни с границами, и доходы от него сравнимы с доходами от торговли оружием или наркотиками.

Компьютерные программы, конфиденциальная электронная информация, электронные деньги стали электронным товаром конца XX и начала XXI веков. До воплощения этого товара в материальную форму, в виде реального товара или денег, его утечка зачастую не обнаруживается, а следовательно, убытки от незаконного использования не явны и трудно определимы, хотя реальный ущерб может исчисляться астрономическими суммами.

Именно поэтому компьютерные преступления чрезвычайно многогранны и сложны. Объектами таких преступных посягательств могут быть сами технические средства (компьютеры и периферия) как материальные объекты или программное обеспечение и базы данных, для которых технические средства являются окружением.

В настоящее время компьютерные преступления чрезвычайно многообразны. Это несанкционированный доступ к информации, хранящейся в компьютере, ввод в программное обеспечение логических бомб, разработка и распространение компьютерных вирусов, хищение компьютерной информации, небрежность в разработке, изготовлении и эксплуатации программно-вычислительных комплексов, подделка компьютерной информации.

Все меры противодействия компьютерным преступлениям, непосредственно обеспечивающих безопасность информации, можно подразделить на:

- правовые;
- организационно-административные;
- инженерно-технические.

К правовым мерам следует отнести разработку норм, устанавливающих ответственность за компьютерные преступления, защиту авторских прав программистов, совершенствование уголовного и гражданского законодательства, а также судопроизводства. К ним относятся также вопросы общественного контроля за разработчиками компьютерных систем и принятие соответствующих международных договоров об ограничениях, если они влияют или могут повлиять на военные, экономические и социальные аспекты стран, заключающих соглашение. Только в последние годы появились работы по проблемам правовой борьбы с компьютерными преступлениями. А совсем недавно и отечественное законодательство встало на путь борьбы с компьютерной преступностью.

К организационно-административным мерам относятся охрана компьютерных систем, подбор персонала, исключение случаев ведения особо важных работ только одним человеком, наличие плана восстановления работоспособности центра после выхода его из строя, обслуживание вычислительного центра посторонней организацией или лицами, не заинтересованными в сокрытии фактов нарушения работы центра, уни-

версальность средств защиты от всех пользователей (включая высшее руководство), возложение ответственности на лиц, которые должны обеспечить безопасность центра, выбор места расположения центра и т. п.

К инженерно-техническим мерам можно отнести защиту от несанкционированного доступа к компьютерной системе, резервирование важных компьютерных систем, обеспечение защиты от хищений и диверсий, резервное электропитание, разработку и реализацию специальных программных и аппаратных комплексов безопасности и многое другое.

Остановимся на них более подробно.

Правовое обеспечение безопасности информации

Правовое обеспечение безопасности информации — это совокупность законодательных актов, нормативно-правовых документов, положений, инструкций, руководств, требования которых обязательны в системе защиты информации. Вопрос о правовом обеспечении безопасности информации в настоящее время активно прорабатывается как в практическом, так и в законотворческом плане.

В качестве инструментов для совершения компьютерных преступлений используются средства телекоммуникаций и вычислительной техники, программное обеспечение и интеллектуальные знания, а сферами их совершения являются не только компьютеры, глобальные и корпоративные сети (Internet/intranet), но и любые области, где используются современные высокопроизводительные средства информационных технологий, там, где обрабатываются большие объемы информации (например, статистические и финансовые институты).

В связи с этим деятельность любого учреждения нельзя представить без процесса получения самой разнообразной информации, ее обработки вручную или с использованием средств вычислительной техники, принятия на основе анализа информации каких-либо конкретных решений и передачи их по каналам связи.

Компьютер может выступать и как сам предмет посягательств, так и как инструмент, с помощью которого оно возможно. Если разделять два последних понятия, то термин «компьютерное преступление» как юридическая категория не имеет особого смысла. Если компьютер — только объект посягательства, то квалифицировать правонарушения можно по существующим нормам права. Если же компьютер только инструмент, то достаточен такой признак, как «применение технических средств». Возможно объединение указанных понятий, когда компьютер одновременно и инструмент, и предмет. В частности, к этой ситуации относится факт хищения машинной информации. •

Если хищение информации связано с потерей материальных и финансовых ценностей, то этот факт можно квалифицировать как преступление. Также если с данным фактом связываются нарушения интересов национальной безопасности, авторства, то уголовная ответственность прямо предусмотрена в соответствии с законами РФ.

Правовое обеспечение безопасности информации любой страны содержит как международные, так и национальные правовые нормы. В нашей стране правовые или законодательные основы обеспечения безопасности компьютерных систем составляют Конституция РФ, Законы РФ, Кодексы, указы и другие нормативные акты, регулирующие отношения в области информации (рис. 3.6).

Предметами правового регулирования являются:

- О правовой режим информации защиты информации;
- О правовой статус участников правоотношений в процессах информатизации;
- ❑ порядок отношений субъектов с учетом их правового статуса на различных стадиях и уровнях процесса функционирования информационных структур и систем.

Рис. 3.6. Правовые нормы обеспечения безопасности информации

Законодательство по информационной безопасности можно представить как неотъемлемую часть всей системы законов Российской Федерации, в том числе:

- ❑ конституционное законодательство, куда нормы, касающиеся вопросов информатизации, входят как составные элементы;
- ❑ общие основные законы (о собственности, недрах, земле, правах граждан, гражданстве, налогах), которые включают нормы по вопросам информатизации;
- ❑ законы по организации управления, касающиеся отдельных структур хозяйства, экономики, системы государственных органов и определяющие их статус. Они включают отдельные нормы по вопросам информации. Наряду с общими вопросами информационного обеспечения деятельности конкретного органа эти нормы должны устанавливать обязанность органа по формированию и актуализации систем и массивов (банков) информации;
- ❑ специальные законы, полностью относящиеся к конкретным сферам отношений, отраслям хозяйства, процессам. В их число входят законы по информатизации — именно состав и содержание этих законов образуют специальное законодательство как основу правового обеспечения информатизации и защиту информации;
- ❑ подзаконные нормативные акты в области информатизации;
- ❑ правоохранительное законодательство РФ, содержащее нормы ответственности за правонарушения в области информатизации.

До недавнего времени, а именно до 1 января 1997 года — даты вступления в действие нового Уголовного Кодекса Российской Федерации (УК РФ) — в России отсутствовала возможность эффективной борьбы с компьютерными преступлениями. Несмотря на явную опасность, данные посягательства не считались противозаконными, то есть о них не упоминалось в уголовном законодательстве. Хотя еще до принятия нового УК в России была осознана необходимость правовой борьбы с компьютерной преступностью. Был принят ряд законов, которые внесли правовую определенность в процесс компьютеризации нашего общества вообще и проблему компьютерной преступности, в частности, и вместе с другими правовыми актами сформировали пакет документов, охватывающий несколько сотен нормативно-правовых актов (в настоящее время отношения в сфере информационной безопасности регулируются более чем 80 законами, иногда достаточно противоречивыми).

Специальное законодательство в области информатизации представляется совокупностью законов, часть из которых уже принята, а часть находится в разработке. Непосредственно законодательство России в области защиты информации и государственных секретов начало формироваться с 1991 года и включало до 1997 года десять основных законов:

- «О средствах массовой информации» (от 27.12.91 г. № 2124—1);
- «Патентный закон РФ» (от 23.09.92 г. № 3517—1);
- «О правовой охране топологий интегральных микросхем» (от 23.09.92 г. № 3526—1);
- «О правовой охране программ для электронных вычислительных машин и баз данных» (от 23.09.92 г. № 3523—1);
- «Основы законодательства об Архивном фонде РФ и архивах» (от 7.07.93 г. № 5341—1);
- «Об авторском праве и смежных правах» (от 9.07.93 г. № 5351—1);
- «О государственной тайне» (от 21.07.93 г. № 5485—1);
- «Об обязательном экземпляре документов» (от 29.12.94 г. № 77—ФЗ);
- «О связи» (от 16.02.95 г. № 15—ФЗ);
- «Об информации, информатизации и защите информации» (от 20.02.95 г. № 24—ФЗ);
- «Об участии в международном информационном обмене» (от 5.06.96 г. № 85—ФЗ).

Кроме этих законов, на первом этапе создания законодательства в этой области были изданы указы Президента Российской Федерации. Вот лишь некоторые из них:

- «О создании Государственной технической комиссии при Президенте Российской Федерации» (от 5.01.92 г. № 9);
- «Концепция правовой информатизации России» (от 23.04.93 г. № 477);
- «О дополнительных гарантиях прав граждан на информацию» (от 31.12.93 г. № 2334);
- «Об основах государственной политики в сфере информатизации» (от 20.01.94 г. № 170);
- «Вопросы защиты государственной тайны» (от 30.03.94 г. № 614);
- О «О совершенствовании деятельности в области информатизации органов государственной власти Российской Федерации» (от 21.04.94 г. № 361);
- «Вопросы деятельности Комитета при Президенте Российской Федерации по политике информатизации» (от 17.06.94 г. № 328);
- «О совершенствовании информационно-телекоммуникационного обеспечения органов государственной власти и порядке их взаимодействия при реализации государственной политики в сфере информатизации» (от 1.07.94 г. № 1390);
- «О мерах по соблюдению законности в области разработки, производства, шифрования информации» (от 3.04.95 г. № 334);
- «Перечень сведений, отнесенных к государственной тайне» (от 30.11.95 г. № 1203);
- «О мерах по упорядочиванию разработки, производства, реализации, приобретения в целях продажи, ввоза в Российскую Федерацию и вывоза за ее пределы, а также использования специальных технических средств, предназначенных для негласного получения информации» (от 9.01.96 г. № 21);
- «Перечень сведений конфиденциального характера» (от 6.03.97 г. № 188).

Среди этих законов особое место занимает базовый закон «Об информации, информатизации и защите информации», в котором заложены основы правового определения всех важнейших компонентов процесса информатизации:

О информатизации и информационных систем;

- субъектов — участников процесса;
- правоотношений производителей — потребителей информационной продукции, владельцев информации;
- обработчиков и потребителей на основе отношений собственности при обеспечении гарантий интересов граждан и государства.

Во всех базовых законах определены цели, объекты, понятия и правовые основы защиты информации (информационных ресурсов). Рассмотрим несколько подробнее Закон РФ «Об информации, информатизации и защите информации», который призван обеспечить соблюдение конституционного права граждан на информацию, ее открытость и доступность, получение гражданами и организациями информации о деятельности органов законодательной, исполнительной и судебной власти и другой информации, представляющей общественный и личный интерес, а также содействовать обращению информации в обществе и развитию информатизации. В нем отражены такие вопросы, как порядок документирования информации и ее включение в информационные ресурсы, право собственности на информационные ресурсы, отнесение информации (информационных ресурсов) к категориям открытого и ограниченного доступа, определение механизмов и полномочий по доступу к информации, порядок правовой защиты информации, механизмы установления ответственности за нарушения в этой сфере и другие. В законе определены основные цели защиты информации:

О предотвращение утечки, хищения, искажения, подделки;

- обеспечение безопасности личности, общества, государства;
- предотвращение несанкционированных действий, направленных на уничтожение, искажение, блокирование информации;
- защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных;
- сохранение государственной тайны, конфиденциальности документированной информации.

Согласно упомянутому закону защите подлежат сведения ограниченного доступа, а степень защиты определяет их собственник. При этом ответственность за выполнение защитных мер лежит не только на собственнике информации, но и на ее пользователе. Поэтому важно четко уяснить: информация, используемая в вашем учреждении, не принадлежит вам, но должна быть обязательно защищена. Причем защищается только документированная информация.

В соответствии с законом документированная информация с ограниченным доступом по условиям ее правового режима подразделяется на:

- государственную тайну (ст. 8);
- конфиденциальную информацию (ст. 10).

К государственной тайне относятся защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб Российской Федерации. Поскольку информацией этой категории вла-

деет само государство, то, естественно, оно же само и выдвигает определенные требования к ее защите, а также контролирует их исполнение. Это оговаривается Законом Российской Федерации 1993 года «О государственной тайне». Нарушения именно этих требований влекут за собой применение санкций, предусмотренных Уголовным Кодексом РФ, по всей строгости законов.

Конфиденциальная информация — это документированная информация, правовой режим которой установлен специальными нормами действующего законодательства в области государственной, коммерческой, промышленной и другой общественной деятельности. Информацией этой категории владеют учреждения и организации, поэтому они вправе ею распоряжаться, а следовательно, и выбирать степень ее защиты. Правда, применить какие-либо санкции в случае нарушения конфиденциальности можно только после предварительного выполнения особых формальностей, оговоренных Гражданским кодексом Российской Федерации.

Суть этих формальностей (ст. 139 Гражданского кодекса РФ) заключается в следующем:

- информация должна иметь действительную или потенциальную коммерческую ценность и эти сведения не могут быть известны третьим лицам в силу каких-либо других условий;
- учреждение принимало определенные меры для исключения на законных основаниях свободного доступа к этой информации и охране ее конфиденциальности;
- все сотрудники, знакомые с этими сведениями, были официально предупреждены об их конфиденциальности.

Только в этом случае закон будет на вашей стороне и вы сможете потребовать возмещения убытков, понесенных от нарушения конфиденциальности информации.

Один из видов конфиденциальной информации — персональные конфиденциальные данные, которыми владеет каждый из нас, т. к. она касается нашей личной жизни. Однако, понимая степень значимости этой информации и ее роль в обеспечении безопасности личности, государство взяло ее под защиту и рассматривает как одну из своих важнейших задач. Правовая сторона этого вопроса на современном этапе еще недостаточно проработана. Только Закон «Об информации, информатизации и защите информации» относит эти сведения к категории конфиденциальных и требует их защиты наравне с информацией, составляющей государственную тайну.

Из всех многочисленных видов конфиденциальной информации в этом законе упомянуты лишь личная и семейная тайны, персональные данные, тайна переписки, телефонных, почтовых, телеграфных и иных сообщений. Однако уже в 1996 году в Федеральном Законе «Об участии в международном информационном обмене» (ст. 8) государственная тайна определяется как конфиденциальная информация. Эта путаница сохраняется во многих законах, где ссылки «на иные охраняемые секреты, иные охраняемые законом тайны» предполагают продолжение списка видов информации с ограниченным доступом.

В Указе Президента РФ от 6.03.97 г. № 188 предпринята попытка упорядочить перечень конфиденциальной информации. В нем утвержден перечень сведений «конфиденциального характера», где указаны 6 видов такой информации:

- персональные данные;
- тайна следствия и судопроизводства;
- служебная тайна;

- ❑ профессиональная тайна;
- ❑ коммерческая тайна;
- ❑ сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

В этих законах определены основные термины и понятия в области компьютерной информации (например, такие как компьютерная информация, программа для ЭВМ, ЭВМ, сеть ЭВМ, база данных и т. п.), регулируются вопросы ее распространения, охраны авторских прав, имущественные и неимущественные отношения, возникающие в связи с созданием, правовой охраной и использованием программного обеспечения и новых информационных технологий. Также раскрываются понятия информационной безопасности и международного информационного обмена. Кроме них, следует также упомянуть Указы Президента РФ, которые касаются, прежде всего, вопросов формирования государственной политики в сфере информатизации (включая организационные механизмы), создания системы правовой информации и информационно-правового сотрудничества с государствами СНГ, обеспечения информацией органов государственной власти, мер по защите информации (в частности, шифрования).

Все эти законы и подзаконные акты в достаточной степени регулировали вопросы охраны исключительных прав и частично защиту информации (в рамках государственной тайны). Не получили достойного отражения в действующем законодательстве права граждан на доступ к информации и защита информации, то есть то, что напрямую связано с компьютерными преступлениями.

Часть указанных пробелов была ликвидирована после введения в действие с 1 января 1997 года нового Уголовного Кодекса, принятого Государственной Думой 24 мая 1996 года. В главе 28 этого Кодекса, которая называется «Преступления в сфере компьютерной информации», приведен перечень признаков, характеризующих общественно опасное деяние как конкретное преступление: составы, компьютерных преступлений:

- О «Неправомерный доступ к компьютерной информации» (ст. 272);
- О «Создание, использование и распространение вредоносных программ для ЭВМ» (ст. 273);
- ❑ «Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети» (ст. 274).

Рассмотрим подробнее все три статьи УК РФ, с целью обрисовать основные признаки совершения компьютерных преступлений, т. е. предусмотренных уголовным законодательством противоправных нарушений, охраняемых законом прав и интересов в отношении компьютерных систем. Сухое описание будет скрашено некоторыми примерами отечественных компьютерных преступлений прошлых лет, компенсирующие бедность правоприменительной практики на базе нового УК РФ.

Итак, статья 272 УК предусматривает ответственность за неправомерный доступ к компьютерной информации (информации на машинном носителе, в ЭВМ или сети ЭВМ), если это повлекло уничтожение, блокирование, модификацию, копирование информации либо нарушение работы вычислительных систем.

Данная статья защищает право владельца на неприкосновенность информации в системе. Владельцем информационной вычислительной системы может быть любое лицо, правомерно пользующееся услугами по обработке информации как собственник вычислительной системы (ЭВМ, сети ЭВМ) или как лицо, приобретшее право использования компьютера.

Преступное деяние, ответственность за которое предусмотрено ст. 272, состоит в неправомерном доступе к охраняемой законом компьютерной информации, который всегда носит характер совершения определенных действий — проникновение в компьютерную систему путем использования специальных технических или программных средств, позволяющих преодолеть установленные системы защиты; незаконного применения действующих паролей или маскировки под видом законного пользователя, хищения носителей информации, при условии, что были приняты меры их охраны, если это деяние повлекло уничтожение или блокирование информации. Неправомерным признается и доступ к защищенной компьютерной информации лица, не обладающего правами на получение и работу с данной информацией либо компьютерной системой.

Неправомерный доступ к компьютерной информации должен осуществляться умышленно. Совершая это, преступник сознает, что неправомерно вторгается в компьютерную систему, предвидит возможность или неизбежность указанных в законе последствий, желает и сознательно допускает их наступление либо относится к этому безразлично.

Мотивы и цели данного преступления могут быть любыми: это и корыстный мотив, цель получить какую-либо информацию, желание причинить вред, желание проверить свои профессиональные способности. Следует отметить правильность действий законодателя, исключившего мотив и цель как необходимый признак указанного преступления, что позволяет применять ст. 272 УК к всевозможным компьютерным посягательствам.

Статья состоит из двух частей. В первой части наиболее серьезное воздействие на преступника состоит в лишении его свободы сроком до двух лет. Один из характерных примеров потенциального применения данной статьи — уголовное дело о хищении 125,5 тыс. долларов США и подготовке к хищению еще свыше 500 тыс. долларов во Внешэкономбанке СССР в 1991 году, рассмотренное московским судом. По материалам другого уголовного дела в сентябре 1993 года было совершено покушение на хищение денежных средств в особо крупных размерах из Главного расчетно-кассового центра Центрального банка России в Москве на сумму 68 млрд рублей. Еще один пример в 1990 году компьютерная программа перечисления комсомольских взносов работников одного из отечественных предприятий была составлена так, что отчисления производились из зарплаты не только комсомольцев, но и всех работников в возрасте до 28 лет. Пострадавших оказалось 67 человек. Теперь это можно квалифицировать по части 1 ст. 272 УК.

Часть вторая ст. 272 предусматривает в качестве признаков, усиливающих уголовную ответственность, совершение его группой лиц либо с использованием своего служебного положения, а равно имеющим доступ к информационной вычислительной системе, и допускает вынесение приговора с лишением свободы до пяти лет.

Ярким примером возможности применения ст. 272 могут служить хорошо освещенные средствами массовой информации действия Владимира Левина и других граждан России, которые вступили в сговор с целью похищения денежных средств в крупных размерах, принадлежащих City Bank of America в Нью-Йорке. Образовав преступную группу, они в период с конца июня по сентябрь 1994 года, используя Internet, проникли в корпоративную сеть «Ситибанка» и, преодолев банковскую сис-

тему защиты от несанкционированного доступа, с помощью персонального компьютера, находящегося в Санкт-Петербурге в офисе акционерного общества «Сатурн», осуществили денежные переводы на общую сумму около 12 млн долларов США.

В разоблачении и задержании электронных мошенников и их сообщников принимали участие представители спецслужб США, Англии, Израиля, Финляндии, Германии и России. Летом 1994 года система безопасности Нью-Йорского отделения «Ситибанка» зафиксировала попытку несанкционированного проникновения в компьютерную сеть банка и сообщила об этом в ФБР. При очередном несанкционированном входе было определено, что проникали в банковскую систему из Санкт-Петербурга. С этого момента операции по перечислению денег находились под полным контролем спецслужб и затем последовали задержания «с поличным». В Сан-Франциско при получении денег были задержаны супруги Корольковы, в Амстердаме — Владимир Воронин, в Израиле — Александр Лашманов. А уже 3 марта 1995 года в Лондоне, в аэропорту Хитроу, был задержан и арестован и сам «мозговой центр» международной преступной группы — Владимир Левин.

В приведенном примере необходимо подчеркнуть следующую немаловажную деталь: состоявшийся в августе 1995 года лондонский суд отложил принятие решения по делу Левина на неопределенный срок, поскольку в ходе судебного разбирательства было доказано, что для получения доступа к счетам клиентов банка подсудимый использовал в качестве орудия преступления компьютер, находящийся на территории России, а не на территории США, как того требует уголовное законодательство Великобритании. На основании вышеизложенного просьба американских и российских представителей о выдаче им Левина была судом отклонена. И только в январе 1998 года он предстал перед судом в Нью-Йорке по обвинению в хищении через Internet денежных средств «Ситибанка».

Тридцатилетний Владимир Левин признал себя виновным в незаконном проникновении в корпоративную сеть «Ситибанка» и переводе со счетов клиентов банка 3,7 млн долларов США на контролируемые им и его сообщниками счета в Финляндии, Нидерландах, Германии, Израиле и США. В итоге он был приговорен к 3 годам тюрьмы и денежному штрафу в размере 240 тыс. долларов США.

В настоящее время действия этой группы лиц можно квалифицировать по ч. 2 ст. 272 УК РФ, так как в результате предварительного сговора ею был осуществлен неправомерный доступ к секретной банковской информации с целью получения материальной выгоды. Местонахождение непосредственного объекта преступления — компьютерная система в США — не повлияло бы на суть дела.

Приведем еще один пример: уголовное дело по обвинению Александра и Бориса Дудровых, которым предъявлено обвинение по ст. 183 УК РФ за незаконное получение и распространение сведений, составляющих коммерческую тайну, по ст. 272 УК РФ за неправомерный доступ к компьютерной информации.

Суть этого дела состоит в следующем. В конце лета 1997 года в адреса различных организаций и коммерческих компаний стала поступать рекламная информация, в которой сообщалось, что компания «Орлов и К°» предлагает к коммерческой продаже различные базы данных с конфиденциальной информацией, анонимные «Голосовые почтовые ящики», телефоны с возможностью программирования ложного телефонного номера. В то же время на рынке стали распространяться лазерные компакт-диски с

базами данных абонентов компаний сотовой связи, базами данных о недвижимости, базой данных о юридических лицах Санкт-Петербурга с указанием подробных сведений об учредителях, виде деятельности и уставном капитале и др. В ходе следствия установлено, что Дудровы (отец и сын) в результате обобщения конфиденциальной информации, полученной из различных источников, создали и распространяли базу данных «Весь Питер», в общей сложности реализовав дисков на сумму более 43 млн неденоминированных рублей. Они приобрели информацию о номерах и кодах доступа к 1000 голосовым почтовым ящикам, которая реализовывалась различным гражданам.

В соответствии со ст. П Закона «Об информации, информатизации и защите информации», вышеуказанные сведения относятся к категории конфиденциальной информации. Дудровы не имели полномочий на нее, нарушали режим защиты, обработки и порядок использования данной информации, а также нарушали условия лицензирования, так как фактически не разрабатывали программное обеспечение, а незаконно ее собирали, адаптировали в программы, пригодные для коммерческого использования, после чего сбывали в Санкт-Петербурге.

Своими действиями Дудровы причинили крупный ущерб государству в виде необоснованной критики в связи с нарушениями порядка сбора, хранения и распространения информации о частной жизни граждан. Кроме того, они допустили свободное использование конфиденциальных баз данных криминальными структурами, тем самым существенно осложнив деятельность правоохранительных органов. Они причинили значительный материальный и моральный вред компаниям сотовой телефонной связи, которые в результате потеряли имидж и, следовательно, потеряли клиентов.

Итогом их деятельности стал суд. В апреле 1999 года Выборгский районный суд Санкт-Петербурга приговорил директора 000 «Орлов и К°» Александра Дудрова к 1 году и 3 месяцам лишения свободы в колонии общего режима, его отца, Бориса Дудрова, работавшего заместителем в той же фирме, и сотрудника «СПб таксофоны» Сергея Аксенова — к 1 году исправительных работ. Правда, всех их тут же амнистировали, но прецедент был создан — впервые суд вынес приговор компьютерным пиратам.

По уголовному законодательству субъектами компьютерных преступлений могут быть лица, достигшие 16-летнего возраста, однако часть вторая ст. 272 предусматривает дополнительный признак у субъекта, совершившего данное преступление, — служебное положение, а равно доступ к ЭВМ, системе ЭВМ или их сети, способствовавших совершению преступления.

Ст. 272 УК не регулирует ситуацию, когда неправомерный доступ осуществляется в результате неосторожных действий, что, в принципе, отсекает много возможных посягательств и даже те действия, которые совершались умышленно, так как при расследовании обстоятельств доступа будет крайне трудно доказать умысел компьютерного преступника (например, в сети Internet, объединяющей миллионы компьютеров, в связи со спецификой работы, при переходе по ссылке от одного компьютера к другому довольно легко попасть в защищаемую информационную зону, даже не заметив этого).

Важна причинная связь между несанкционированным доступом и наступлением предусмотренных ст. 272 последствий, поэтому простое временное совпадение момента сбоя в компьютерной системе, которое может быть вызвано неисправностями или программными ошибками, и неправомерного доступа не влечет уголовной ответственности.

Ст. 273 УК защищает права владельца компьютерной системы на неприкосновенность находящейся в ней информации и предусматривает уголовную ответственность за создание программ для ЭВМ или их модификацию, заведомо приводящее к несанкционированному уничтожению, блокированию и модификации данных, либо копированию информации, нарушению работы информационных систем, а равно использование таких программ или носителей таких программ.

Вредоносные программы в смысле ст. 273 УК РФ — это программы, специально разработанные для нарушения нормального функционирования компьютерных систем. Под нормальным функционированием понимают выполнение определенных в документации на программу операций. Наиболее распространены компьютерные вирусы и логические бомбы.

Для привлечения к ответственности по ст. 273 необязательно наступление каких-либо отрицательных последствий для владельца информации, достаточен сам факт создания программ или внесения изменений в существующие программы, заведомо приводящих к негативным последствиям, перечисленным в статье. Использование программ — это выпуск в свет, воспроизведение, распространение и иные действия по их введению в информационный обмен. Использование может осуществляться путем записи в память ЭВМ, на материальный носитель, распространения по сетям либо передач другим лицам иным путем.

Уголовная ответственность по этой статье возникает уже в результате создания программы, независимо от того, использовалась она или нет. По смыслу ст. 273 наличие исходных текстов вирусных программ уже есть основание для привлечения к ответственности. Следует учитывать, что в ряде случаев использование подобных программ не будет уголовно наказуемым. Это относится к деятельности организаций, разрабатывающих антивирусные программы и имеющих соответствующую лицензию.

Данная статья состоит из двух частей, отличающихся друг от друга признаком отношения преступника к совершаемым действиям. Преступление, предусмотренное частью 1 ст. 273, может быть совершено только умышленно, с сознанием того, что создание, использование или распространение вредоносных программ заведомо должно привести к нарушению неприкосновенности информации. Причем цели и мотивы не влияют на квалификацию посягательства по данной статье, поэтому самые благородные побуждения (например, борьба за экологическую чистоту планеты) не исключают ответственности за само по себе преступное деяние. Максимально тяжелым наказанием для преступника в этом случае будет лишение свободы до трех лет.

Часть вторая ст. 273 в качестве дополнительного квалифицирующего признака предусматривает наступление тяжких последствий по неосторожности. При совершении преступления, предусмотренного частью 2 рассматриваемой статьи, лицо сознает, что создает вредоносную программу, использует либо распространяет такую программу или ее носители и либо предвидит возможность наступления наказания, но без достаточных к тому оснований самонадеянно рассчитывает на его предотвращение, либо не предвидит этих последствий, хотя при необходимой внимательности и предусмотрительности должно и могло их предусмотреть. Данная норма закономерна, поскольку разработка вредоносных программ доступна только квалифицированным программистам; они в силу своей профессиональной подготовки должны предвидеть потенци-

ально возможные последствия использования этих программ, которые могут быть весьма многообразными: смерть человека, вред здоровью, возникновение реальной опасности военной или иной катастрофы, нарушение функционирования транспортных систем. По этой части суд может назначить максимальное наказание в виде семи лет лишения свободы.

В 1983 году на одном автомобильном заводе нашей страны был изобличен программист, который из мести к руководству предприятия умышленно внес изменения в программу ЭВМ, управлявшей подачей деталей на конвейер. В результате произошедшего сбоя заводу был причинен материальный ущерб: не сошло с конвейера свыше сотни автомобилей. Программист был привлечен к уголовной ответственности. Подсудимый обвинялся по ст. 98 ч. 2 Уголовного кодекса РСФСР «Умышленное уничтожение или повреждение государственного или общественного имущества... причинившее крупный ущерб». При этом обвиняемый утверждал, что ничего натурально повреждено не было — нарушенным оказался лишь порядок работы, то есть действия, не подпадающие ни под одну статью действующего в то время законодательства. С научной точки зрения интересен приговор суда: «Три года лишения свободы условно; взыскание суммы, выплаченной рабочим за время вынужденного простоя главного конвейера; перевод на должность сборщика главного конвейера».

В настоящее время квалификация действий этого программиста должна была бы производиться по ч. 1 ст. 273. Он умышленно создал и использовал в заводском компьютере вредоносную программу, нарушившую технологический процесс. Но если видоизменить проводимый мысленный эксперимент: по неосторожности (допустим, из-за конфликта программного и аппаратного обеспечения) действие программы привело к тяжким последствиям — гибели людей на конвейере. Тогда, несомненно, указанные действия квалифицируются уже по ч. 2 ст. 273. А если убрать «неосторожность» и считать, что преступник действовал умышленно, то тогда оказывается, что в этом случае за тяжкие последствия по ст. 273 отвечать не нужно.

Как свидетельствуют материалы одного уголовного дела, сотрудник отечественной АЭС из корыстных побуждений использовал в системах управления станцией несанкционированные программные модули. В итоге это привело к искажению информации, отображаемой на пульте оператора атомного реактора, повлекшее возникновении нештатной ситуации, последствия которой не нуждаются в пояснении. Отсюда закономерно сделать вывод о том, что формулировку данной статьи следует изменить.

Если же в действиях лица содержатся не только признаки преступления, предусмотренного ст. 273 УК, но и признаки другого преступления (убийства, уничтожения имущества), виновный будет нести ответственность по совокупности совершенных преступлений.

Статья 274 УК устанавливает ответственность за нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ним, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации, если это деяние причинило существенный вред.

Статья защищает интерес владельца вычислительной системы относительно ее правильной эксплуатации. В ней охраняемой законом информацией считается информация, для которой в специальных законах установлен режим ее правовой защиты.

Однако между фактом нарушения и наступившим существенным вредом должна быть установлена причинная связь и полностью доказано, что наступившие последствия являются результатом именно нарушения правил эксплуатации. Определение существенного вреда, предусмотренного в данной статье, устанавливается судом в каждом конкретном случае, исходя из обстоятельств дела, однако очевидно, что существенный вред должен быть менее значительным, чем тяжкие последствия.

Преступник, нарушивший правило эксплуатации, — это лицо, в силу должностных обязанностей имеющее доступ к компьютерной системе и обязанное соблюдать установленные для этой системы технические правила.

Кроме того, преступник должен совершать свое деяния умышленно, он должен сознавать, что нарушает правила эксплуатации, предвидя возможность или неизбежность неправомерного воздействия на информацию и причинение существенного вреда, желает или сознательно допускает причинение такого вреда или относится к его наступлению безразлично. Что наиболее строго наказывается лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет.

Данная уголовная норма, естественно, не содержит конкретных технических требований и отсылает к ведомственным инструкциям и правилам, определяющим порядок работы, которые должны устанавливаться специально уполномоченным лицом и доводиться до пользователей. Применение данной статьи невозможно для Internet, ее действие распространяется только на локальные сети организаций.

В части второй статьи 274 предусматривается ответственность и за неосторожные деяния. По ней должны квалифицироваться, например, действия специалиста по обслуживанию системы управления транспортом, установившего инфицированную программу без антивирусной проверки, повлекшее серьезную транспортную аварию.

По данным правоохранительных органов, имеются сведения о фактах несанкционированного доступа к ЭВМ вычислительного центра железных дорог России, а также к электронной информации систем учета жилых и нежилых помещений местных органов управления во многих городах, что в наше время подпадает под ответственность, предусмотренную ст. 272 УК, либо ст. 274 УК в зависимости от действий лица, осуществившего посягательство, и правил эксплуатации конкретной сети.

Следует отметить, что признаки преступлений, предусмотренных в статьях 272 и 274 УК, с технической точки зрения весьма похожи. Различие заключается в правомерности или неправомерности доступа к ЭВМ, системе ЭВМ или их сети. Статья 274 УК отсылает к правилам эксплуатации конкретной компьютерной системы, а в статье 272 УК в качестве одного из последствий указывается нарушение работы компьютерной системы, что, с технической точки зрения, является отступлением от правил и режима эксплуатации.

Подводя некоторые итоги, можно сделать вывод о том, что сложность компьютерной техники, неоднозначность квалификации, а также трудность сбора доказательственной информации не приведет в ближайшее время к появлению большого числа уголовных дел, возбужденных по статьям 272-274 УК.

Предусмотренные составы компьютерных преступлений не охватывают полностью всех видов совершения компьютерных посягательств. В этом случае будут оказывать помощь статьи 146 УК РФ (нарушение авторских и смежных прав), 147 УК РФ

(нарушение изобретательских и патентных прав), и 155 (незаконное использование товарных знаков), дающие возможность уголовного преследования за незаконное использование программного обеспечения.

17 марта 1998 года Экономический отдел РУОП Санкт-Петербурга провел крупномасштабную операцию по пресечению фактов незаконного оборота контрафактного программного обеспечения. Этой операции предшествовали сотрудничество с Ассоциацией производителей программного обеспечения (Business Software Alliance, BSA), тщательный сбор информации об объектах реализации контрафактной продукции, компьютерное исследование образцов пиратской продукции. Кроме того, была получена поддержка и заявления компаний «Проект МТ», «1С», «Фирмы БИТ» о нарушении их авторских прав. На основании собранных материалов накануне операции прокуратура завела уголовное дело по ст. 142 ч. *2* УК РФ по фактам нарушения авторских прав, и были получены санкции на проведение следственных действий.

Сами пираты окрестили день 17 марта 1998 года как «черный вторник». В результате операции было изъято около 24 000 компакт-дисков со сборниками программных продуктов различных компаний-производителей, на которых находилось порядка 500 тыс. программных продуктов на сумму около 30 млн долларов США.

В период с 15 по 30 октября 1998 года в Москве была произведена проверка торговых комплексов, отдельных фирм и торговых точек. В результате проверок было обнаружено и изъято более 400 тыс. нелицензионных компьютерных дисков и заведено несколько уголовных дел по ст. 146 УК РФ.

К правовому обеспечению относятся и такие формы, как составление договоров на проведение работ и на оказание информационных услуг. Здесь правовая гарантия предусматривается определенными условиями ответственности за нарушение сторонами принятых обязательств (помимо возмещения убытков, возможны штрафные санкции).

Кроме этих гарантий, стороны могут застраховаться от убытков. Тогда они в договоре определяют, какая именно сторона заключает договор страхования со страховой компанией, а также случаи возникновения убытков, подлежащих страхованию. Как правило, страхование берет на себя исполнитель, но тогда страховая сумма учитывается при определении суммы договора.

В условиях неразвитого государственного правового механизма обеспечения безопасности компьютерных сетей серьезное значение приобретают документы предприятия, регулирующие отношения с государством и с коллективом сотрудников на правовой основе. К таким основополагающим документам, которые также играют важную роль в обеспечении безопасности, можно отнести:

- устав предприятия (фирмы, банка), закрепляющий условия обеспечения безопасности деятельности и защиты информации;
- коллективный договор;
- трудовые договоры с сотрудниками предприятия, содержащие требования по обеспечению защиты сведений, составляющих коммерческую тайну и др.;
- правила внутреннего трудового распорядка рабочих и служащих;
- должностные обязанности руководителей, специалистов и обслуживающего персонала.

Организационно-административное обеспечение безопасности информации

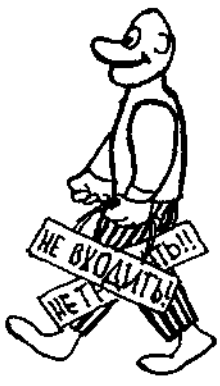
По мнению специалистов, организационные мероприятия играют важную роль в создании надежного механизма защиты информации, так как возможности несанкционированного использования конфиденциальных сведений в значительной мере обуславливаются не техническими аспектами, а злоумышленными действиями, нерадивостью, небрежностью и халатностью пользователей или персонала, игнорирующего элементарные правила защиты.

Организационное обеспечение (рис. 3.7) — это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе таким образом, что разглашение, утечка и несанкционированный доступ к конфиденциальной информации становится невозможным или существенно затрудняется за счет проведения организационных мероприятий.

Влияния этих аспектов практически невозможно избежать с помощью технических средств, программно-математических методов и физических мер. Для этого необходима совокупность организационно-правовых и организационно-технических мероприятий, которые исключали бы (или по крайней мере сводили к минимуму) возможность возникновения опасности для информации.

К организационным мероприятиям можно отнести:

- мероприятия, осуществляемые при проектировании, строительстве и оборудовании служебных и производственных зданий и помещений (их цель — исключение возможности тайного проникновения на территорию и в помещения; обеспечение удобства контроля прохода и перемещения людей, проезда транспорта; создание отдельных производственных зон по типу конфиденциальности работ с самостоятельными системами доступа и т. п.);
- мероприятия, проводимые при подборе персонала, включающие ознакомление с сотрудниками, их изучение, обучение правилам работы с конфиденциальной информацией, ознакомление с мерами ответственности за нарушение правил защиты информации и др.;
- организацию и поддержание надежного пропускного режима и контроля посетителей;
- надежную охрану помещений и территории;
- хранение и использование документов и носителей конфиденциальной информации, включая порядок учета, выдачи, исполнения и возвращения;
- организацию защиты информации, т. е. назначение ответственного за защиту информации в конкретных производственных коллективах, проведение систематического контроля за работой персонала с конфиденциальной информацией, порядок учета, хранения и уничтожения документов и т. п.



В каждом конкретном случае такие мероприятия носят специфическую для данной организации форму и содержание, направленные на обеспечение безопасности информации в конкретныхусловиях.

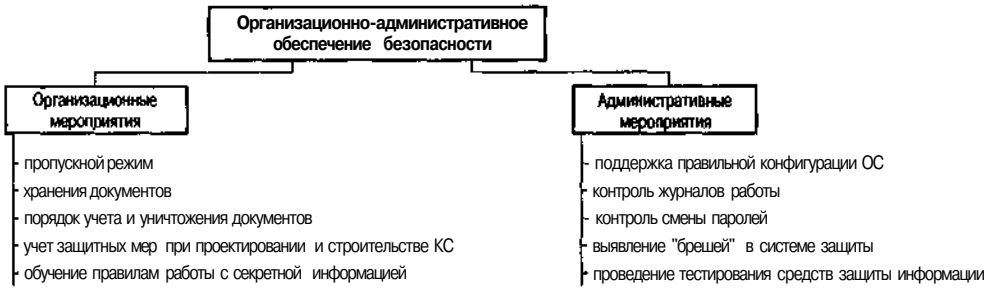


Рис. 3.7. Основные организационные и административные мероприятия по защите информации в сети

Очевидно, что организационные мероприятия охватывают самые различные источники информации и технические средства ее переработки. Значительная доля организационных мероприятий приходится на работу с сотрудниками. Организационные мероприятия при работе с сотрудниками предприятий различных форм собственности в общем плане включают в себя:

О беседы при приеме на работу;

- ознакомление с правилами и процедурами работы с конфиденциальной информацией на данном предприятии;
- обучение сотрудников правилам и процедурам работы с конфиденциальной информацией;
- беседы с увольняемыми.

В результате беседы при приеме на работу устанавливается целесообразность приема кандидата на соответствующую вакансию. При приеме на работу возможно заключение между предприятием и сотрудником соглашения о неразглашении конфиденциальной информации, которая является собственностью организации.

В подтверждение требований сохранения в тайне коммерческой информации поступающий на работу сотрудник дает подписку о сохранении коммерческой тайны предприятия и обязуется не раскрывать секреты фирмы.

Обучение сотрудников предполагает не только приобретение и систематическое поддержание на высоком уровне производственных навыков, но и психологическое их воспитание в глубокой убежденности, что необходимо выполнять требования промышленной (производственной) секретности, информационной безопасности, защиты интеллектуальной собственности и коммерческой тайны. Систематическое обучение способствует повышению уровня компетентности руководства и сотрудников в вопросах защиты коммерческих интересов своего предприятия.

Беседы с увольняющимися имеют главной целью предотвратить разглашение информации или ее неправильное использование. В ходе беседы следует особо подчеркнуть, что каждый увольняющийся сотрудник имеет твердые обязательства о неразглашении фирменных секретов и эти обязательства, как правило, подкрепляются подпиской о неразглашении известных сотруднику конфиденциальных сведений.

Одним из важных направлений мероприятий является четкая организация системы делопроизводства и документооборота, которая обеспечивает порядок делопроизвод-

ства, порядок учета, обработки, хранения, уничтожения и контроля наличия и правильности исполнения документов. При реализации системы особое внимание нужно уделять безопасности документов и конфиденциальной информации.

Организационные мероприятия по защите информации предусматривают:

- обеспечение безопасности рабочих зданий и территории;
- обеспечение безопасности отдельных зон и конкретных помещений;
- организацию четкой системы контроля допуска и доступа на территорию (в помещение), к определенной информации.

Документирование информации проводится по строго определенным правилам. Основные из них изложены в ГОСТ 6.38-90 «Система организационно-распорядительной документации. Требования к оформлению документов», ГОСТ 6.10.4-84 «Унифицированные системы документации. Придание юридической силы документам на машинном носителе и машинограмме, создаваемым средствами вычислительной техники» и некоторых других. Надо отметить, что эти ГОСТы предполагают 31 реквизит, которые делают информацию документом, но не обязательно, чтобы присутствовали все предлагаемые реквизиты. Главный реквизит — это текст. Поэтому любая информация, изложенная в виде связного текста без каких-либо дополнительных реквизитов, уже может рассматриваться как документ, для придания определенной юридической силы которому необходимы такие важные реквизиты, как дата и подпись.

Особый порядок существует только для документов, полученных из автоматизированных информационных систем. При этом, в определенных случаях, применяется процедура заверения электронной подписью информации, полученной от удаленного объекта.

Основные организационные мероприятия — разработка перечня охраняемых сведений и проведение аттестации помещений на предмет выработки конкретных мер для защиты конфиденциальной информации. При аттестации помещений составляют аттестационные паспорта. Эта работа производится группами специалистов, оформляется актом, прикладываются соответствующие рекомендации и отдается приказ по организации, где указаны конкретные исполнители и сроки реализации.

Для защиты информации требуется создать специальную административную службу, обеспечивающую все организационные мероприятия. Ее штатная структура, численность и состав определяется реальными потребностями фирмы, степенью конфиденциальности ее информации и общим состоянием безопасности.

Защита информации — удовольствие достаточно дорогое, поэтому одним из принципов построения системы защиты должно стать дифференцирование степени защиты по ее важности и ценности.

Анализ мирового и отечественного опыта обеспечения безопасности говорит о необходимости создания целостной системы безопасности учреждения, связывающей организационные, оперативные и оперативно-технические меры защиты с использованием современных методов прогнозирования, анализа и моделирования ситуаций.

Важным дополнением организационных мероприятий является поддержка правильной конфигурации сетевой операционной системы. Решают такую задачу, как правило, системные администраторы.

Администратор создает определенные правила, которые должны соблюдаться уже не людьми, а операционной системой. Администрирование системы — это правиль-

ное составление файлов конфигурации. В этих файлах (а их может быть несколько, например, по одному файлу для каждой части системы) и содержится описание правил функционирования системы.

Административное обеспечение очень дешево, т. к. средства расходуются только на содержание специалиста (причем один специалист способен управлять сразу несколькими системами). Более того, большинством современных систем можно управлять удаленно.

Обучение пользователей при этом требуется самое минимальное. Обычно система сама не даст пользователю произвести запрещенные действия, он просто видит, что какое-либо действие в системе просто не получается. Если административными мерами закрыт определенный порт соединения, то слабая с точки зрения безопасности программа ICQ не сможет соединиться со своим сервером и, как следствие, не будет функционировать.

Уязвимость системы кроется в том, что, во-первых, система аутентификации пользователя базируется на имени пользователя и его пароле (имеются в виду общеупотребительные системы, экзотические случаи вроде использования сетчатки глаза в расчет не берутся), а во-вторых, в необходимости наличия в системе пользователя, наделенного правом администрировать систему — супервизора (supervisor).

Достаточно нарушить режим хранения пароля супервизора и вся система окажется доступна для несанкционированного воздействия. Кроме того, система, основанная на таких правилах, — это статичная, закостенелая система. Она способна противостоять лишь строго определенным атакам. При возникновении какой-либо новой угрозы, не предусмотренной изначально, сетевая атака может быть не просто успешной, но и оказаться невидимой для системы. Пользователи должны уяснить для себя два несложных правила:

- даже зная пароль супервизора, не следует вмешиваться в дела системных администраторов;
- системные файлы, созданные в процессе администрирования, играют важную роль в системе безопасности корпоративных сетей, поэтому не следует трогать эти файлы, а уж тем более, удалять.

Чтобы свести к минимуму риск в коммерческой деятельности, нужно оценивать всевозможные угрозы безопасности с учетом двух факторов:

- возможной частоты угроз;
- возможного ущерба от них.

Поэтому очень важно четко уяснить, какая используемая в вашем учреждении информация, пусть даже не принадлежащая вам, подлежит обязательной защите. Начать надо с проведения предварительного анализа имеющейся информации. От этого в дальнейшем будет зависеть выбор степени ее защиты. Все это позволит дифференцировать мероприятия по обеспечению безопасности информации и, тем самым, сократить расходы.

При организации защиты информации необходимо придерживаться определенного курса, следуя некоторым советам:

- проанализируйте информацию, которая циркулирует в вашем учреждении;
- определите сведения ограниченного доступа;
- оцените коммерческую важность информации;

- составьте перечень сведений, содержащих коммерческую тайну, утвердите его и ознакомьте с ним исполнителей;
- определите объем информации, составляющей государственную или коммерческую тайну;
- убедитесь в лояльности сотрудников службы безопасности;
- принимая сотрудника на работу, постарайтесь, всеми доступными средствами, навести о нем справки;
- продумайте систему морального и материального поощрения сотрудников за соблюдение секретности;
- регулярно тестируйте сотрудников, которые имеют дело с информацией ограниченного доступа;
- обязательно оговаривайте в договоре или контракте с сотрудником условия сохранения служебных тайн не только на период совместной работы, но и на определенный срок после завершения ваших взаимоотношений;
- старайтесь всегда соблюдать принцип комплексного подхода к решению проблемы защиты информации;
- придерживайтесь правила «доверяй, но проверяй» (появится уверенность, что в критический момент система безопасности не даст сбоя);
- учитывайте пространственные факторы: введение контролируемых (охраняемых) зон, правильный выбор помещений и расположение объектов между собой и относительно границ контролируемой зоны;
- учитывайте временные факторы: ограничение времени обработки защищаемой информации, доведение времени обработки информации с высоким уровнем конфиденциальности до узкого круга лиц;
- создайте концепцию информационной безопасности;
- увяжите эту концепцию с общей концепцией безопасности вашего учреждения.

Принятие организационных мер по обеспечению безопасности информации ложится в первую очередь на администраторов сети и специалистов по защите информации. Выявить вмешательство в компьютерную систему часто трудно вследствие того, что злоумышленникам удается скрыть следы проникновения в систему. Все попытки взлома систем обнаруживаются, как правило, совершенно случайно. Например, администратор сети заметил пропуск в файле протокола или вхождение в систему в отсутствие пользователя. Или он был предупрежден другими администраторами безопасности о присутствии постороннего в сети.

Обычно злоумышленники действуют в нерабочее время (с 18.00 до 8.00), а также в выходные и праздничные дни. Поэтому для выявления несанкционированного доступа необходимо:

- регулярно проверять файлы протоколов, особенно протоколов входа в систему;
- отслеживать подсоединение неизвестных пользователей в непривычное время;
- обращать внимание на идентификаторы пользователей, которые оставались какое-то время неиспользованными и оказались снова задействованными.

Одним из способов выявления постороннего присутствия в сети является запуск каждые 10 мин обычной shell-процедуры, фиксирущей все процессы и соединения по сети в отдельном файле. Эта программа формирует списки пользователей, всех текущих процессов и сетевых подключений.

Сегодня на рынке средств защиты представлены разнообразные системы защиты информации. Перед администратором безопасности встает вопрос определения необходимости и порядка их применения. Очевидно, что далеко не все компьютеры организации нужно оснащать дополнительными системами защиты информации, так как это требует новых материальных затрат и может только затруднить эксплуатацию всей компьютерной сети в целом.

Применение средств защиты информации целесообразно при:

- О размещении на компьютерах средств криптографической защиты данных (здесь дополнительные средства защиты информации необходимы для защиты ключей электронной цифровой подписи и шифрования);
- О необходимости регламентации и протоколирования действий пользователей, работающих на компьютерах, подключенных к сети (в этом случае система защиты не позволяет пользователям действовать так, как не предусмотрено технологией обработки данных);
- ❑ необходимости ограничения доступа пользователей, работающих на компьютере, к его локальным ресурсам (дискам, каталогам, файлам или внешним устройствам), а также исключения самостоятельного изменения состава и конфигурации программных средств, установленных на компьютере.

Применение дополнительных средств защиты предполагает выполнение администратором безопасности ряда действий. Он должен:

- ❑ устанавливать средства защиты информации на компьютеры;
- ❑ настраивать средства защиты информации путем задания прав доступа пользователей к ресурсам (как компьютеров, так и сети);
- ❑ контролировать состояние защищенности компьютерной сети путем оперативного мониторинга и анализа системных журналов.

В большинстве случаев средства защиты информации устанавливаются на уже реально функционирующую систему. Поскольку защищаемая компьютерная система обычно используется для решения важных задач (часто в непрерывном технологическом цикле), ее владельцы и пользователи неодобрительно относятся к любому, даже кратковременному, перерыву в ее работе, необходимому для установки и настройки системы защиты информации.

Следует учитывать, что с первого раза правильно настроить систему защиты практически невозможно. Обычно это связано с отсутствием полного детального списка всех аппаратных, программных и информационных ресурсов системы, подлежащих защите, и готового противоречивого перечня прав доступа и полномочий каждого пользователя. Поэтому этап внедрения системы защиты информации обязательно включает первоначальное выявление, последовательное уточнение и соответствующее изменение настроек, устанавливаемых в этой системе.

Очевидно, что те же самые действия администратору безопасности придется неоднократно повторять и на этапе эксплуатации системы защиты информации при изменениях состава технических средств, программного обеспечения и т. д. Такие изменения происходят довольно часто, поэтому средства управления этой системы должны обеспечивать удобство осуществления необходимых при этом настроек.

В случае, если средства управления не приспособлены к этому, а сами системы защиты информации не обладают достаточной гибкостью, то очень скоро они стано-

вятся не помощником, а обузой для всех и, в первую очередь, — для администраторов безопасности. В конце концов такие системы защиты информации обречены на отторжение.

Деятельность администратора безопасности на этапе эксплуатации системы защиты информации состоит в корректном и своевременном изменении полномочий пользователей и настройке защитных механизмов на компьютерах сети. С увеличением масштаба защищаемой компьютерной сети и при сохранении неизменным количества людей, отвечающих за ее информационную безопасность, изменяются требования к способам управления этой системой. Как показывает практика, решения, приемлемые для одного компьютера или небольшой сети из 10—15 рабочих станций, обычно не устраивают обслуживающий персонал и администраторов безопасности больших сетей, объединяющих сотни машин.

Проблемы по управлению полномочиями пользователей и настройками системы защиты информации в компьютерной сети могут быть решены, например, на основе использования системы централизованного управления доступом к сети.

Принцип реализации такой системы состоит в применении специального сервера управления доступом, работающего на основном файловом сервере сети, который осуществляет автоматическую синхронизацию центральной базы данных защиты с локальными базами данных защиты, размещенных на рабочих станциях.

Введение распределенной базы данных защиты (центральной и локальных) гарантирует, что выход из строя сети или сервера управления доступом не будет препятствовать нормальному функционированию средств защиты на рабочих станциях.

При данной системе управления доступом полномочия пользователя меняются периодически и заносятся в центральную базу данных защиты, а их изменение на конкретных компьютерах происходит во время очередного сеанса синхронизации.

Кроме того, при смене пользователем своего пароля на одной из рабочих станций его новый пароль автоматически отражается в центральной базе данных защиты, а также передается на рабочие станции, на которых данному пользователю разрешено работать.

Администратору безопасности необходимо контролировать состояние компьютерной сети как оперативно (путем слежения за состоянием защищенности компьютеров сети), так и не оперативно (путем анализа содержимого журналов регистрации событий системы защиты информации).

Использование сервера управления доступом для оперативного контроля за состоянием рабочих станций и работой пользователей позволяет отказаться от постоянного администратора безопасности. В этом случае сервер управления доступом автоматически регистрирует несанкционированные действия, происходящие в сети, и всегда обладает оперативной информацией о состоянии рабочих станций.

Увеличение количества рабочих станций и использование программных средств, включающих много разнообразных компонентов, приводит к существенному увеличению объемов журналов регистрации событий в системе защиты информации. Объем сведений, хранящийся в журналах, может стать настолько большим, что администратор уже физически не сможет полностью проанализировать их содержимое за приемлемое время.

Зашита от компьютерных вирусов в настоящее время основывается на применении организационных мероприятий и программных средств, которые практически вклю-

чают в себя аппаратные возможности компьютеров, программных средств, системного программного обеспечения и специальных программных средств защиты.

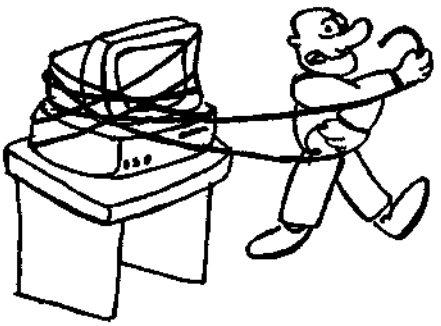
Организационные средства также позволяют минимизировать риск заражения компьютеров вирусами, а при заражении — сразу же информировать пользователя и помочь уничтожить вирус и его последствия. Организационные меры защиты включают следующие основные мероприятия:

- резервирование (наличие всех основных компонентов операционной системы и программного обеспечения в архивах, копирование таблиц распределения файлов дисков, ежедневное ведение архивов изменяемых файлов);
- профилактика (систематическая выгрузка содержимого активной части винчестера на дискеты, раздельное хранение компонентов программного обеспечения и программ пользователей, хранение неиспользуемых программ в архивах);
- ревизия (обследование вновь получаемых программ на дискетах и дисках на наличие вирусов, систематическая проверка длин файлов, хранящихся на винчестере, использование и постоянная проверка контрольных сумм при хранении и передаче программного обеспечения, проверка содержимого загрузочных секторов винчестера и используемых дискет системных файлов);
- фильтрация (разделение винчестера на логические диски с различными возможностями доступа к ним, использование резидентных программных средств слежения за файловой системой);
- защита, основанная на применении специальных программных средств.

Все эти мероприятия, в той или иной степени, включают использование различных программных средств защиты. К их числу необходимо отнести программы-архиваторы, программы резервирования важных компонентов файловой системы, просмотра содержимого файлов и загрузочных секторов, подсчета контрольных сумм и собственно программ защиты.

Инженерно-техническое обеспечение безопасности информации

В настоящее время для получения конфиденциальной информации злоумышленниками, в том числе и промышленными шпионами, используются самые разнообразные средства и способы проникновения на объекты, разработанные на основе последних достижений науки и техники, с использованием новейших технологий в области миниатюризации в интересах скрытного их использования. Для противодействия этому натиску службы безопасности оснащаются необходимой аппаратурой, не уступающей по надежности и функциональным возможностям аппаратуре злоумышленников. Инженерно-техническое обеспечение безопасности информации путем осуществления необходимых технический и организационных мероприятий должно исключать:



- неправомочный доступ к аппаратуре обработки информации путем контроля доступа в производственные помещения;
- неправомочный вынос носителей информации персоналом, занимающимся обработкой данных, посредством выходного контроля в соответствующих производственных помещениях;
- несанкционированное введение данных в память, изменение или стирание информации, хранящейся в памяти;
- неправомочное пользование системами обработки информации и незаконное получение в результате этого данных;
- доступ в системы обработки информации посредством самодельных устройств и незаконное получение данных;
- возможность неправомочной передачи данных через компьютерную сеть;
- бесконтрольный ввод данных в систему;
- обработку данных заказчика без соответствующего указания последнего;
- неправомочное считывание, изменение или стирание данных в процессе их передачи или транспортировки носителей информации.

Методы защиты информации от большинства угроз базируются на инженерных и технических мероприятиях (рис. 3.8). Инженерно-техническая защита — это совокупность специальных органов, технических средств и мероприятий, функционирующих совместно для выполнения определенной задачи по защите информации.

Инженерно-техническая защита использует следующие средства:

- физические средства;
- аппаратные средства;
- программные средства;
- криптографические средства.

Физические средства включают в себя различные инженерные средства и сооружения, препятствующие физическому проникновению злоумышленников на объекты защиты и защищающие персонал (личные средства безопасности), материальные средства и финансы, информацию от противоправных действий.

По уровню физической защиты все зоны и производственные помещения могут быть подразделены на три группы:

- тщательно контролируемые зоны с защитой высокого уровня;
- защищенные зоны;
- слабо защищенные зоны.

К первой группе относятся, как правило, серверные комнаты, помещения с сетевым и связным оборудованием, архив программ и данных.

Ко второй группе относятся помещения, где расположены рабочие места администраторов, контролирующих работу сети, а также периферийное оборудование ограниченного пользования.

В третью группу входят помещения, в которых оборудованы рабочие места пользователей и установлено периферийное оборудование общего пользования.

К аппаратным средствам относятся приборы, устройства, приспособления и другие технические решения, используемые в интересах обеспечения безопасности. В практике деятельности любой организации находит широкое применение самая различная аппаратура: от телефонного аппарата до совершенных автоматизированных

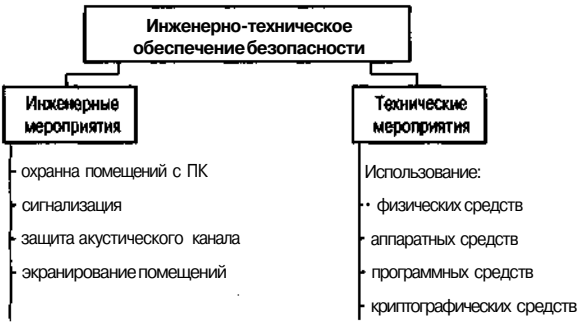


Рис. 3.8. Основные инженерные и технические мероприятия по защите информации в сети

информационных систем, обеспечивающих ее производственную деятельность. Основная задача аппаратных средств — стойкая безопасность коммерческой деятельности.

Программные средства — это специальные программы, программные комплексы и системы защиты информации в информационных системах различного назначения и средствах обработки данных.

Криптографические средства — это специальные математические и алгоритмические средства защиты информации, передаваемой по сетям связи, хранимой и обрабатываемой на компьютерах с использованием методов шифрования.

Очевидно, что такое деление средств безопасности информационных систем достаточно условно, так как на практике очень часто они и взаимодействуют и реализуются в комплексе в виде программно-аппаратной реализации с широким использованием алгоритмов закрытия информации. Например, в настоящее время для обеспечения безопасности передачи данных в компьютерных сетях применяются следующие механизмы защиты информации:

- идентификация и аутентификация;
- управление доступом;
- обеспечение конфиденциальности данных и сообщений;
- обеспечение целостности данных и сообщений;
- контроль субъектов взаимодействия;
- регистрация и наблюдение.

Следует отметить, что назначение указанных выше механизмов может быть разнообразным. Некоторые из них предназначены для уменьшения риска угроз, другие обеспечивают защиту от этих угроз, третьи их обнаруживают. При этом для каждого из механизмов важную роль играют методы криптографии, позволяющие создавать более совершенные средства защиты.

При создании системы физической безопасности (как и информационной безопасности вообще) должен стать анализ угроз (рисков) как реальных (в данный момент), так и потенциальных (в будущем).

По результатам анализа рисков с использованием средств оптимизации формируются требования к системе безопасности конкретного предприятия и объекта в конк-

ретной обстановке. Завышение требований приводит к неоправданным расходам, занижение — к возрастанию вероятности реализации угроз.

В общем случае система физической безопасности должна включать в себя следующие подсистемы:

- управления доступом (с функцией досмотра);
- обнаружения проникновения, аварийной и пожарной сигнализации (тревожной сигнализации);
- инженерно-технической защиты (пассивной защиты);
- отображения и оценки обстановки;
- управления в аварийных и тревожных ситуациях;
- оповещения и связи в экстремальных ситуациях;
- обеспечения личной безопасности персонала.

При построении системы физической безопасности, удовлетворяющей сформулированным требованиям, выбираются и объединяются средства противодействия из числа указанных ниже:

- здания и строительные препятствия, мешающие действиям злоумышленника и задерживающие его;
- аппаратура тревожной сигнализации, обеспечивающая обнаружение попыток проникновения и несанкционированных действий, а также оценку их опасности;
- системы связи, обеспечивающие сбор, объединение и передачу тревожной информации и других данных;
- системы управления, необходимые для отображения и анализа тревожной информации, а также для реализации ответных действий оператора и управления оборонительными силами;
- персонал охраны, выполняющий ежедневные программы безопасности, управление системой и ее использование в нештатных ситуациях;
- процедуры обеспечения безопасности, предписывающие определенные защитные мероприятия, их направленность и управление ими.

В свою очередь, технические методы защиты информации подразделяются на:

- аппаратные;
- программные;
- аппаратно-программные.

Остановимся на следующих направлениях обеспечения безопасности информации (с ориентацией на электронно-вычислительную технику):

- защита от несанкционированного доступа к информации в компьютерных системах и сетях;
- антивирусная защита;
- предотвращение перехвата через нежелательные электромагнитные и акустические поля и излучения;
- обеспечение высокой структурной скрытности сообщений на основе криптографических методов.

Более подробно мы рассмотрим эти вопросы в следующих главах этой книги.

Определение степени защищенности сети

Компьютерная сеть любой современной организации — это разнородная многокомпонентная система. Защита одного или нескольких компонентов не может обеспечить необходимый уровень защищенности информационных ресурсов предприятия, что в современной сложной обстановке, когда различные негативные проявления типа вирусных атак стали обычным повседневным явлением, — настоятельная потребность.

Разумеется, компьютерной сети угрожают не только вирусы, здесь можно отметить сбои, остановки в работе, ошибки в программах, конфликты периферийных устройств, «дыры» в операционных системах и другие вредоносные факторы. Кроме того, вопросами обеспечения безопасности часто начинают заниматься тогда, когда информационное пространство объекта уже сформировалось. Между тем, любая информация — ценнейший товар предприятия. Ее потеря из-за неэффективно организованной защиты может обернуться серьезными финансовыми проблемами для ее собственника.

Большинство пользователей сети предприятия (фирмы) являются профессионалами в различных областях, но не владеют в достаточной мере специальными знаниями в области защиты информации для оценки уровня безопасности сети. Если кто-либо из них, возможно, сможет грамотно сконфигурировать сложно настраиваемый комплекс, использовать специализированные прикладные программы, осуществлять администрирование сети, то многие не справятся с несложными операциями подключения внешних устройств. Поэтому даже в том случае, когда элементы комплекса средств защиты полностью или частично внедрены, вопрос, насколько они эффективны, остается актуальным. Для решения этого вопроса не всегда необходимо прибегать к таким дорогостоящим и требующим значительных временных затрат средствам, как сертификационная процедура оценки по требованиям безопасности.

Современные требования, предъявляемые к защищенным компьютерным системам, изложены в документе, имеющем статус международного стандарта, который получил название «Общие критерии» (Common Criteria for Information Technology Security Evaluation. Version 1.0) и появился совсем недавно, отличаются большей гибкостью, динамизмом по сравнению с предшествующими. При этом подход, основанный на разработке подобных требований к информационным системам и дальнейшей оценке соответствия им, можно считать наиболее приемлемым.

В настоящее время существует несколько методов оценки защищенности компьютерных сетей (рис. 3.9). Среди них можно выделить:

- аналитический;
- имитационный;
- экспертный.

Ни один из этих методов не имеет преимущества над другим. При выборе и использовании методов и моделей той или иной группы следует опираться только на их соответствие решаемой задаче и применять те методы, которые в данной ситуации наиболее оправданы.

Что касается самого метода оценки защищенности, то здесь можно сказать следующее. Действительно, с методической точки зрения аналитические и имитационные

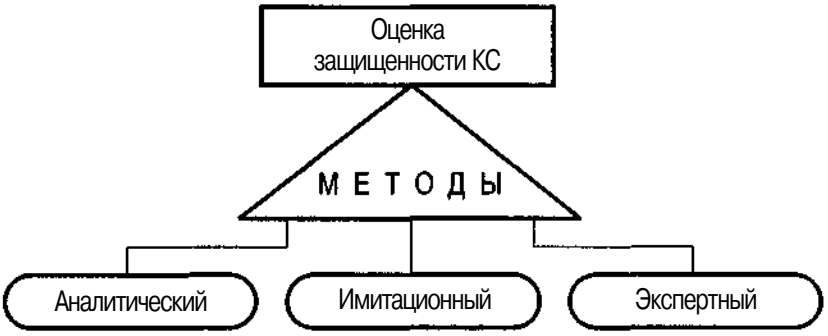


Рис. 3.9. Методы оценки защищенности компьютерных сетей

модели, которые разработаны к настоящему времени, выглядят более предпочтительными, так как основываются на формализованном представлении предметной области. Экспертные методы позволяют находить решение в условиях слабоструктурированной предметной области.

Однако отметим, что существующие на сегодняшний день модели и методики оценки во многом ориентированы на узкого специалиста-профессионала, который хорошо разбирается в данной конкретной проблематике. Что же касается вопроса определения необходимого набора требований и критериев оценки и их соблюдения, то здесь основная трудность состоит в сложности выработки полного и достоверного их множества и повторяющемся характере процедуры их конкретизации в течение всего жизненного цикла компьютерной сети. И эта трудность до сих пор не преодолена. Кроме того, найти компромисс между стремлением проектировщиков систем защиты к конкретности требований и совместимости их с современными типами архитектур локальных и распределенных сетей и желанием пользователей получить простую, однозначную и в то же время гибкую систему требований, определяющих защищенность, очень трудно. А с учетом роли специалистов-оценщиков, требующих детально регламентировать процедуру квалификационного анализа и максимально четко определить совокупность критериев оценки и их значения, ситуация достижения компромисса становится практически нереальной.

Поэтому при решении задачи анализа защищенности компьютерной сети целесообразно сформировать группу специалистов-экспертов различного профиля (метод экспертной оценки), которые будут взаимодействовать с заказчиком (пользователем, проектировщиком) и корректировать требования в соответствии с их непониманием решаемых задач. Таким образом, процессы оценки качества функционирования сети с точки зрения безопасности будут органически вписываться в сценарий проектирования и эксплуатации компьютерной сети, а руководство предприятия и его ведущие специалисты смогут активно участвовать в этом процессе. Эксперты же, руководствуясь опытом и знаниями, смогут подсказать, на что следует обратить внимание, и ответить на вопрос, связанный с возможностью эксплуатации оцениваемой компьютерной сети с учетом обеспечиваемого уровня защищенности, который оправдан с точки зрения важности охраняемой и обрабатываемой средствами данной сети информации. Сама же оценка защищенности будет выполнять сразу несколько функций:

- аналитическую, которая включает тщательное и всестороннее изучение сетевой структуры, ее элементов, внешней среды, в которой она функционирует;
- контрольную, связанную с выработкой требований к разработке, внедрению и эксплуатации средств защиты;
- консультативно-диагностическую, ориентированную на анализ состояния системы защиты сети, формирование рекомендаций по предпочтению и использованию механизмов, обеспечивающих защищенность.

Применение метода экспертных оценок не является новым для решения задач в различных областях.

Например, в медицине довольно часто практикуется сопоставление мнений ведущих специалистов, когда необходимо поставить диагноз и определить способ лечения пациента в случаях особо сложных заболеваний. Аналогично этому, в отношении задачи оценки защищенности компьютерной сети можно провести некоторую аналогию. Здесь при анализе механизмов, обеспечивающих защищенность, эксперт ставит своего рода диагноз, дающий ответ на вопрос о возможности использования данной системы для обработки конфиденциальной информации. При этом мнение одного специалиста может оказаться совершенно отличным от мнения другого, так как разные эксперты могут детально разбираться каждый в своей, достаточно узкой, профессиональной области. Объединение, сопоставление и анализ результатов оценки различных специалистов позволяют получить более полную картину относительно объекта экспертизы.

Такой методический подход как раз и способствует выявлению широкого диапазона мнений специалистов в данной предметной области и получению на этой базе объективного экспертного заключения о защищенности оцениваемой компьютерной сети. Кроме того, при данном подходе возможно проведение экспертного анализа собственными силами предприятия, активно использующего средства информатизации. Это, конечно, не означает, что необходимость в специализированной оценке, осуществляемой сегодня специальными государственными структурами на основе соответствующих стандартов и нормативных документов, практически отпадает. Однако благодаря предварительному анализу защищенности по предлагаемой процедуре может уменьшиться вероятность повторного обращения в специализированные центры, в случае, когда принято решение о том, чтобы подвергнуть локальную сеть сертификационной процедуре.

При выборе показателей оценки защищенности компьютерной сети должны учитываться следующие принципы:

- ясность и измеряемость значений;
- отсутствие перекрытия между используемыми показателями;
- соответствие установившимся понятиям и терминологии;
- возможность последующего уточнения, дополнения и детализации.

Каждый показатель может принимать значения типа: «высокая», «средняя», «низкая», «полное соответствие», «частичное» и т. д. Такая формулировка создает достаточно удобства для работы эксперта, так как ему предлагается оценить степень соответствия фактического и требуемого состояния системы защиты сети по некоторым важным параметрам.

Системы выявления атак на сеть

Всемирная сеть Internet растет с головокружительной скоростью, поэтому нет ничего удивительного в том, что регистрируется все больше попыток несанкционированного доступа к корпоративным ресурсам. Планы таких атак не являются тайной, так что часто их можно найти прямо в готовом для применения формате, а недавние эксцессы, носившие поистине глобальный характер, — явное свидетельство того, что в целом совершить компьютерное преступление сегодня намного проще, чем раньше. И если прежде основную угрозу представлял тщательно организованный промышленный шпионаж, то теперь ему на смену приходят «воришки со сценариями», «проказы» которых, возможно, обойдутся вашей компании в тысячи долларов из-за простоя в результате проведения несложной, стандартной скрытой атаки.

Конечно, это не то, на чем можно сделать фильм о Джеймсе Бонде, но результаты могут оказаться столь же драматичными. Ежегодные убытки от атак на компьютерные сети составляют десятки и даже сотни миллионов долларов.

Прошли те времена, когда простой брандмауэр был достаточно надежным средством защиты, чтобы администраторы сетей могли спокойно спать. Современные корпорации предусматривают сложные стратегии защиты, реализация которых предполагает использование нескольких систем, как предупредительных, так и реактивных (часто они являются многоуровневыми и избыточными). В этом новом мире Internet выявление атак становится столь же распространенным, как шифрование и аутентификация. Оно широко применяется крупными и мелкими компаниями.

Суть систем выявления атак проста и состоит в установке агентов для проверки сетевого трафика и поиска сигнатур известных сетевых атак. Однако с развитием сетевых вычислений и пугающим распространением Internet все несколько усложнилось. С появлением распределенных атак по типу отказ в обслуживании (Distributed Denial of Service, DDoS), часто инициируемых из сотен различных источников, адрес отправителя трафика больше не может служить надежным свидетельством того, что против вас не организована атака. Хуже того, адекватно реагировать на такие атаки становится все труднее из-за разнообразия исходных систем, особенно из-за того, что большинство атак по своей природе географически распределены.

Администраторы сети ведут со злоумышленниками трудную борьбу, и в этой связи возможность распознавать некоторые (если не все) атаки в тот момент, когда они происходят, себя оправдывает, поскольку это позволяет своевременно предпринять корректирующие действия.

Потенциальных злоумышленников, покушающихся на вашу интеллектуальную собственность, много. Важно знать не только, как правильно реагировать на инцидент, но и как идентифицировать злоумышленников (рис. 3.10).

Выявить же злоумышленника в основном не представляет особой сложности по следующим его действиям:

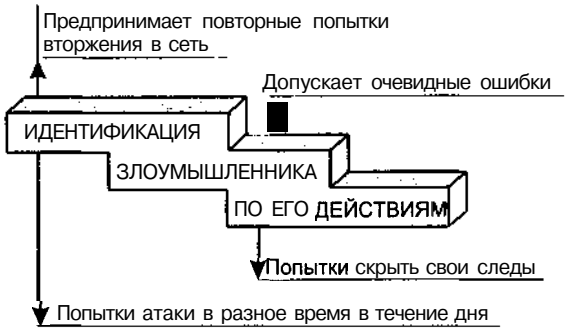


Рис. 3.10. Идентификация злоумышленника по его действиям

О предпринимает повторные попытки вторжения в сеть;
- ❑ допускает очевидные ошибки;
- ❑ предпринимает попытки атаки в разное время в течение дня;
- ❑ хочет скрыть свои следы.

В случае неудачной попытки доступа к серверу случайные злоумышленники оставят вас в покое. С другой стороны, опытные злоумышленники постараются собрать информацию о сервере, чтобы вернуться позже и попытаться использовать другие слабости. Например, в один прекрасный день при просмотре журналов IDS вы обращаете внимание на то, что кто-то сканирует ваш почтовый сервер в поисках открытых портов TCP и UDP. Двумя днями позже IP-адрес злоумышленника всплывает вновь, но на этот раз злоумышленник нацеливается на открытые порты. Несколько часов спустя он вводит последовательность команд SMTP через порт 25.

Каждое нажатие клавиши во время атаки дает ценную информацию об опыте атакующего. Серьезный хакер не позволит себе терять драгоценное время на синтаксические ошибки и метод проб и ошибок. Попытка ввести команды SMTP через порт NNTP служит ясным свидетельством неопытности атакующего.

Картина доступа может дать такие важные сведения о злоумышленнике, как его местонахождение, профессия и возраст. Большинство случайных атакующих осуществляют свои попытки между 9 часами вечера и 1 часом ночи. Если попытки проникновения имеют место по будним дням с 9 утра до 5 вечера, то наверняка они производятся с рабочего места.

Были ли случаи, когда при проверке системных журналов событий вы обнаруживали, что все записи за последние 12 часов пропали? Когда-либо замечали, что файл истории команд для бюджета root таинственно исчез? Это признаки опытного атакующего. Он позаботился об удалении всех свидетельств своих действий, не опасаясь, что это приведет к подаче тревожного сигнала. Такое поведение аналогично действиям грабителя, поджигающего дом перед тем, как бежать оттуда с награбленным.

Существенную помощь администратору в данном случае могут оказать системы выявления атак.

Хотя системы выявления атак до сих пор считаются экспериментальными, они стали значительно совершеннее с момента первого их использования (1988 г.), причем до

такой степени, что они заняли свое собственное место в системе обороны сети наравне с брандмауэрами и антивирусным программным обеспечением. Хотя практические реализации таких систем, как правило, достаточно сложны и нестандартны, общая концепция выявления атак на удивление проста и состоит в проверке всей активности сети (как входящей, так и исходящей) и обнаружении подозрительных действий, которые могли бы свидетельствовать об атаке на сеть или систему. Эффективность выявления атак на сеть может быть повышена при выполнении последовательности операций, которые представлены на рис. 3.11.

Большинство имеющихся на рынке инструментальных средств выявления атак использует две фундаментальные методики:

- ❑ выявление злоупотреблений;
- ❑ выявление аномалий.

Выявление злоупотреблений опирается на предопределенный набор сигнатур (шаблонов) атак, которые могут быть получены у производителя или указаны сетевым администратором. Выполняя поиск конкретных шаблонных действий, системы выявления атак, пытаются установить соответствие каждого из поступающих в сеть пакетов сигнатуре известной атаки. Очевидные преимущества данной методики — ее простота и необременительность (как следствие, нет трудностей и при развертывании). Однако, у этого подхода есть существенный недостаток: проверка каждого пакета в сети становится все сложнее, особенно с учетом последних достижений сетевой технологии.

Администраторы защиты должны хорошо подготовиться, прежде чем приступить к выбору системы выявления злоупотреблений. Обязательно поинтересуйтесь у производителя, как часто появляются новые сигнатуры атак и сколько стоит обновление службы. Как и в вопросе обнаружения вирусов, полезность программного обеспечения напрямую зависит от полноты базы данных с сигнатурами, которую оно использует при анализе пакетов.

Выявление аномалий наиболее полезно в стабильных сетевых средах, где администратор может легко определить нормальное состояние сети в таких терминах, как уровень трафика, отказ протокола и типичный размер пакета. Детекторы аномального поведения можно настроить таким образом, чтобы они периодически проводили мониторинг сетевых сегментов и определенного числа сетевых серверов и сравнивали их состояние с основным. Если эти состояния значительно различаются, то могут быть

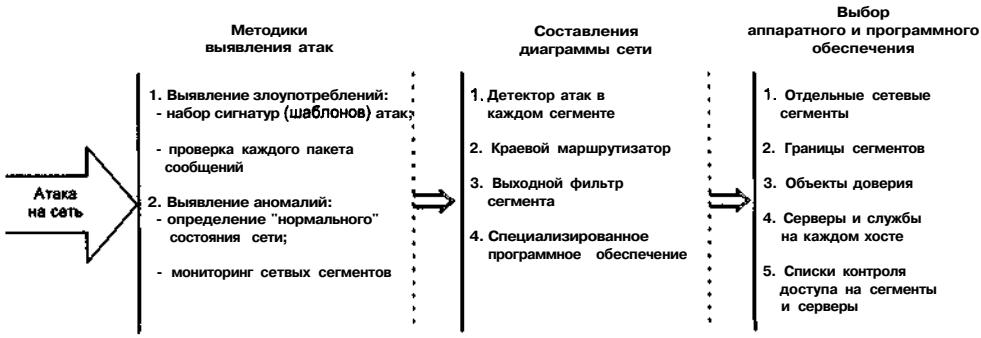


Рис. 3.11. Последовательность операций для эффективного выявления атак на сеть

предприняты соответствующие действия. Например, если в два часа дня в воскресенье уровень загруженности вашего сегмента в демилитаризованной зоне (Demilitarized Zone, DMZ) внезапно увеличивается до 80%, причем 90% пакетов этого трафика являются эхопакетами протокола управляющих сообщений ICMP (Internet Control Message Protocol) на запросы от различных источников, то весьма вероятно, что ваша сеть подверглась атаке DDoS.

Большая часть систем выявления атак использует сочетание обеих методик, и они часто устанавливаются в сети, на конкретном хосте или даже для конкретного приложения на хосте.

Наверное, самое очевидное место для размещения системы выявления атак — непосредственно в том сегменте, контроль за которым вы хотите установить. Сетевые детекторы атак устанавливаются в сети точно так же, как и любое другое устройство, за исключением того, что они проверяют все пакеты, которые видят. Хотя системы выявления атак достаточно просты в реализации и развертывании, они все же не лишены недостатков, о которых стоит упомянуть.

Во-первых, действительно разделяемые сегменты (на базе концентраторов, а не коммутаторов) сейчас встречаются довольно редко, т. е. для мониторинга всей подсети одного датчика недостаточно. Вместо этого системы выявления атак должны быть интегрированы в определенный порт коммутаторов Ethernet (с поддержкой режима приема всех пакетов), что не всегда возможно, даже если такой порт имеется.

Кроме того, при обслуживании всего сегмента одной системой выявления атак она становится уязвимой для атаки DDoS. Если злоумышленник сможет вывести из строя сам детектор, то он получает полную свободу действий и может проникнуть в подсеть, не опасаясь быть обнаруженным. Об этой опасности всегда следует помнить при проектировании и установке хоста для своей системы выявления атак. Как и брандмауэр, такая система не должна:

- содержать пользовательские бюджеты, за исключением привилегированного пользователя (root/Administrator); поддерживать необязательные сетевые службы;
- предлагать никакой вид интерактивного сетевого доступа (доступ возможен только через консоль);
- работать под управлением малоизвестной, нестандартной операционной системы.

Если система выявления атак размещается на стандартной многозадачной, многопользовательской системе, то это должен быть укрепленный вариант операционной системы, где не инициируется (и не размещается) большинство пользовательских процессов, чтобы она могла обеспечить необходимую производительность для проверки каждого пакета по мере их поступления. Это освобождает машину от необязательной нагрузки по обработке и позволяет сосредоточиться на выполнении поставленной задачи.

Если ваша политика защиты такова, что злонамеренное вторжение будет иметь серьезные негативные последствия для вашего бизнеса, то рекомендуется установить избыточные системы выявления атак. В идеале эти системы нужно приобретать у двух производителей или, по крайней мере, устанавливать на двух различных платформах. Смысл в том, чтобы не класть все яйца в одну корзину. (Конечно, концепция избыточности применима ко всем подобным системам.)

Хотя такой подход предполагает дополнительные затраты на поддержку разнородного аппаратного обеспечения и операционных систем, вы можете легко компенсировать этот недостаток, выбрав системы выявления атак, управление которыми может осуществляться централизованным и защищенным образом с помощью стандартных инструментальных средств для управления сетями и системами.

Еще одна часто реализуемая стратегия в отношении выявления атак на сеть состоит в автоматическом блокировании доступа по всему периметру сети в случае выхода из строя системы выявления атак. О случившемся необходимо немедленно сообщить администратору сетевой защиты, так как он может оценить создавшуюся ситуацию и предпринять необходимые корректирующие действия. Отметим, что это решение зачастую предполагает, что система выявления атак должна взаимодействовать с размещенными по периметру сети устройствами, такими как брандмауэры и краевые маршрутизаторы.

Как это часто бывает в сложном мире сетевой защиты, панацеи не существует, и, чтобы стратегия выявления атак была эффективной, она должна быть реализована на нескольких уровнях. Установка и обслуживание сетевых детекторов для выявления атак трудностей не вызывают, однако это не позволяет выявить целый класс атак, опознать которые крайне сложно, так как они тесно связаны с целевой системой. Эти атаки используют уязвимые места конкретных операционных систем и пакетов приложений. Только системы выявления атак на хост могут отслеживать сложный массив специфичных для систем параметров, совокупность которых составляет сигнатуру хорошо организованной атаки (такие системы работают как приложения на подключенном к сети хосте).

Ориентированный на хосты подход идеален для серверов высокой доступности, которые предприятия используют в своей повседневной работе. Эти серверы, как правило, в любом случае устанавливаются в «слабозаселенных» сегментах, так что дополнительные расходы на размещение на хосте детекторов не должны создать непреодолимых трудностей. Возможно, самое важное преимущество этого подхода в том что он позволяет выявить внутренние операции, т. е. обнаружить ситуацию, когда законопослушный пользователь обращается с ресурсами хоста таким образом, что это ведет к нарушению принятой в компании политики защиты. Такого рода нарушения практически невозможно обнаружить посредством системы выявления атак на сеть, поскольку пользователь может обращаться к системе с консоли, и передаваемые им команды просто не пересылаются по сети.

Однако и в деле выявления атак на хост тоже не все гладко. Поскольку эти системы тесно связаны с операционной системой, они становятся еще одним приложением, которое необходимо обслуживать и переносить. Это весьма важный момент в среде, где операционные системы часто обновляются, поскольку система выявления атак может работать эффективно, только тогда, когда она имеет все последние данные. Кроме того, сама по себе установка детекторов на хосты не защитит вашу компанию от базовых атак DDoS на сетевом уровне (SYN flooding, ping of death, land attack и т. д.). Но, несмотря на эти ограничения, система выявления атак на хосты должна стать неотъемлемой частью общей защиты от вторжений.

Развитие методов выявления атак привело к развитию имеющихся систем обнаружения тщательно подготовленных атак. Функционируя на самом верху сетевого стека (на прикладном уровне), эти системы выполняют мониторинг конкретных приложе-

ний (например, серверы Web, электронной почты и баз данных) в поисках подозрительных шаблонов и для анализа сообщений из журналов приложений.

Детекторы атак на приложения постоянно проверяют журнальные файлы и системные переменные в поисках готовящейся атаки. Хотя они представляют собой полезные, нужные механизмы, ориентированные на приложения системы трудны в управлении и реализации, так как критически важным сетевым приложениям каждого вида требуется своя система выявления атак. Они должны стать последним рубежом защиты от тех изощренных атак, которые их инициаторы сумели достаточно хорошо замаскировать, чтобы обмануть системы выявления атак на сеть и хосты.

Идея установки программного обеспечения выявления атак на маршрутизаторах всегда воспринималось со значительной долей скепсиса, так как проверка каждого пакета в поисках сигнатуры атаки обычно отнимает значительную часть общей производительности маршрутизатора. Однако маршрутизаторы обладают прекрасной возможностью распознавания и предотвращения атак еще до того, как они проникнут внутрь корпоративной сети, где ущерб от них может оказаться намного существеннее.

Реализованная на маршрутизаторе простая методика фильтрации позволяет гарантировать, что ваша компания не станет стартовой точкой для организации атаки DDoS. Применяемые при этом так называемые выходные фильтры представляют собой набор правил для проверки исходящих пакетов и анализа адресов их отправителей. Поскольку используемые с внутренней стороны краевого маршрутизатора сетевые адреса, как правило, известны, маршрутизаторы могут отфильтровывать пакеты, чьи адреса отправителей не соответствуют их сетям.

Это позволяет фильтровать потенциально подделанный трафик, обычно наблюдаемый, когда злоумышленники захватывают ничего не подозревающий хост и отправляют с него пакеты на выбранную ими цель где-нибудь в Internet. Многие провайдеры стали реализовывать выходные фильтры на всем управляемом ими оборудовании в помещениях заказчика (Customer Premises Equipment, CPE).

Как только вы выбрали аппаратное и программное обеспечение для обнаружения атак, следующий шаг в реализации эффективной системы выявления атак — составление диаграммы всей сети, в которой четко указаны пять элементов:

- ❑ отдельные сетевые сегменты;
- ❑ границы сегментов;
- ❑ заслуживающие и не заслуживающие доверия объекты;
- ❑ все серверы (хосты) и службы, работающие на каждом хосте;
- ❑ списки контроля доступа ACL (Access Control List) на границе каждого сегмента и на каждом сервере.

Отдельные сетевые сегменты — к примеру, от маршрутизатора к маршрутизатору, вместе со списком сетевых протоколов и типичной нагрузкой, которая, по вашему мнению, будет характерна для каждого сегмента.

Границы сегментов — это маршрутизаторы, коммутаторы и брандмауэры.

Заслуживают **и** не заслуживают доверия известные локальные и удаленные пользователи, партнеры по бизнесу, анонимные пользователи и потенциальные клиенты электронной коммерции.

И число инцидентов, и диапазон злонамеренных сетевых атак продолжают расти, в силу чего время реакции на подобные инциденты становится критически важным. Из-

за нехватки специалистов по защите все больший интерес в отрасли вызывают автоматизированные системы реакции на атаку, с помощью которых система выявления атак может сразу предпринять оборонительные (или, по крайней мере, сдерживающие) меры в ответ на вторжение.

Распространенная ошибка при проектировании автоматизированных систем реакции на атаку состоит в том, что такие системы часто делают именно то, на что рассчитывает злоумышленник.

К примеру, рассмотрим политику защиты, при которой система выявления атак отфильтровывает адрес отправителя, с которого, по имеющейся информации, производится сканирование портов хостов в вашей сети. В действительности злоумышленник достаточно просто может выдать себя за другой хост (подделав IP-адрес), что, в конечном итоге, приведет к фильтрации пакетов ни в чем не повинного хоста (возможно, одного из ваших партнеров по бизнесу или, хуже того, потенциального заказчика). В этом случае злоумышленник, по сути, использует вашу автоматизированную систему противодействия для проведения атаки по типу «отказ в обслуживании» и против вашей сети, и против хоста, за который он себя выдает.

Вместо того чтобы отказывать в доступе подозреваемому в организации атаки, часто полезнее получить больше информации о хосте, с которого производится атака: можно попытаться отследить маршрут до хоста организатора атаки, провести обратный поиск DNS по IP-адресу злоумышленника, постараться выяснить тип хоста (определить тип ОС) и установить провайдера Internet инициатора вторжения.

Собранная информация позволит принять более взвешенное решение о том, что следует сделать: отказать в доступе по всему периметру, предупредить администратора или просто зарегистрировать событие как подозрительное. Не забудьте записать всю собранную информацию (предпочтительно через Syslog) на удаленный хост, где эти данные можно сохранить на вторичной системе хранения.

Целостность журналов и других критически важных системных файлов может быть гарантирована с помощью инструментальных средств обеспечения целостности системных файлов. Этот инструментарий периодически вычисляет контрольные суммы для данных, находящихся в журналах регистрации, хранимых в безопасном месте. Контрольные суммы затем регулярно пересчитываются и сравниваются с оригиналом, обеспечивая таким образом **неповрежденность** журнальных файлов.

Кроме того, ваша политика защиты должна предусматривать периодический анализ журналов для выявления подозрительной активности. Анализ файлов регистрации и синтаксический разбор в реальном времени позволяют проводить целый ряд соответствующих инструментальных средств (как коммерческих, так и свободно распространяемых). Они способны помочь администратору систем защиты в решении этой рутинной задачи.

При реализации технологии выявления атак администраторы систем защиты должны помнить о двух основных ее недостатках:

- маскировки (evasion);
- вставки (insertion).

Сетевые детекторы используют стандартные или определенные пользователями сигнатуры, которые они пытаются обнаружить в передаваемых по сети пакетах. Однако опытный злоумышленник может замаскировать сигнатуру своей атаки, разбив один TCP-пакет

на несколько IP-пакетов. Чтобы не попасться на эту удочку, убедитесь, что детектор атак в состоянии собирать фрагменты пакетов для анализа сигнатур в реальном времени.

Вторая проблема состоит в добавлении злоумышленником ложных пакетов в TCP-диалог. Несмотря на то, что конечный хост просто отвергнет лишний пакет, детектор атак попытается его проанализировать. Если конечный хост проверяет порядковый номер TCP, дабы убедиться, что пакеты транспортного уровня прибывают в правильном порядке, то детектор вторжений, как правило, эту последовательность не отслеживает и примет за реальные такие фальшивые пакеты, как запрос на прерывание соединения. При получении фальшивого запроса на закрытие (типа TCP FIN), детектор будет игнорировать все остальные пакеты в данном потоке, поскольку он будет уверен, что конечный хост тоже их игнорирует. (Он считает, что соединение уже было закрыто.)

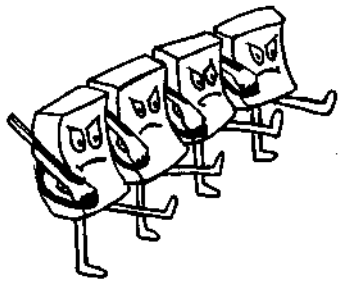
Проявляющиеся сейчас в области межсетевых взаимодействий тенденции потребуют, вероятно, серьезного пересмотра механизма современных систем выявления атак. Технологии виртуальных частных сетей предусматривают внедрения пакетов внутрь других пакетов, а технология шифрования делает практически невозможными проникновение в эти пакеты и проверку сигнатуры атаки.

Кроме того, сетевые шлюзы все чаще и чаще рассчитаны на коммутацию пакетов более высоких уровней со скоростью их поступления и принимают решения о направлении пакетов на основе лишь определенных фрагментов в заголовке пакета. Выявление атак станет, скорее всего, серьезным препятствием на пути повышения скорости коммутаторов до многих гигабит. Производители признают, что они больше не в состоянии предлагать порт для перехвата всех пакетов без значительного снижения производительности коммутирующего оборудования. Одно из возможных решений этой проблемы состоит в реализации распределенных систем выявления атак с несколькими коллекторами с единой высокопроизводительной базой данных, сервер которой имеет достаточную производительность для консолидации всей информации практически в реальном времени. С другой стороны, производители сетевого оборудования могли бы встраивать некоторый небольшой по размеру (хотелось бы надеяться, что стандартный) код выявления атак в архитектуру коммутаторов.

Развертывание эффективных систем выявления атак представляет собой сложную задачу, но она кажется тривиальной по сравнению с тем временем и усилиями, которые вам придется потратить, чтобы обеспечить ту отдачу, на которую рассчитывала ваша компания, в том числе на предпродажные исследования и постоянные модернизации сигнатур атак. Администратору систем защиты не стоит ждать легкой жизни, но он, безусловно, будет спокойнее спать, зная, что в вечно бодрствующем мире Internet корпоративная сеть имеет недремлющего стража.

Программы обнаружения сетевых атак

Злоумышленники редко бесцеремонно вторгаются в сеть с «оружием» в руках. Они предпочитают проверить, надежны ли запоры на двери и все ли окна закрыты. Они незаметно анализируют образцы трафика, входящего в вашу сеть и исходящего из нее, отдельные IP-адреса, а также выдают внешне нейтральные запросы, адресованные отдельным пользователям и сетевым устройствам.



Для обнаружения этих искусно закамуфлированных врагов приходится устанавливать интеллектуальное программное обеспечение детектирования сетевых атак, обладающее высокой чувствительностью. Приобретаемый продукт должен предупреждать администратора не только о случаях явного нарушения системы информационной безопасности, но и о любых подозрительных событиях, которые на первый взгляд кажутся совершенно безобидными, а в действительности скрывают полномасштабную хакерскую атаку. Нет нужды доказывать, что о всякой активной попытке взлома системных паролей администратор должен быть извещен немедленно.

Современные корпорации находятся буквально под перекрестным огнем со стороны злоумышленников, стремящихся похитить ценные сведения или просто вывести из строя информационные системы. Задачи, преследуемые в борьбе с хакерами, достаточно очевидны:

- уведомление о предпринятой попытке несанкционированного доступа должно быть немедленным;
- отражение атаки и минимизация потерь (чтобы противостоять злоумышленнику, следует незамедлительно разорвать сеанс связи с ним);
- переход в контрнаступление (злоумышленник должен быть идентифицирован и наказан).

Именно такой сценарий использовался при тестировании четырех наиболее популярных систем выявления сетевых атак из присутствующих сегодня на рынке:

- BlackICE;
- Intruder Alert;
- Centrax;
- eTrust Intrusion Detection.

Характеристика указанных программных систем обнаружения сетевых атак приведена в табл. 3.2.

Программа BlackICE фирмы Network ICE — специализированное приложение-агент, предназначенное исключительно для выявления злоумышленников. Обнаружив непрошеного гостя, оно направляет отчет об этом событии управляющему модулю ICEcap, анализирующему информацию, поступившую от разных агентов, и стремящемуся локализовать атаку на сеть.

Программное обеспечение Intruder Alert компании Alert Technologies больше похоже на инструментарий для специалистов в области информационной безопасности, поскольку оно предоставляет максимальную гибкость в определении стратегий защиты сети.

Пакет Centrax производства CyberSafe устроен по принципу «все в одном»: в его составе есть средства контроля за системой безопасности, мониторинга трафика, выявления атак и выдачи предупреждающих сообщений.

Система eTrust Intrusion Detection корпорации Computer Associates особенно сильна функциями контроля за информационной безопасностью и управления стратегиями защиты, хотя и в этом продукте реализованы средства вьщачи предупреждений в режиме реального времени, шифрования данных и обнаружения атак.

Таблица 3.2. Характеристика программных систем обнаружения сетевых атак

Программная система	Производитель	Характеристика системы
BlackICE (специализированное приложение-агент)	Network ICE	Устанавливается на компьютере удаленного пользователя или на узле корпоративной сети. Выдает предупреждение об атаке на экран монитора пользователя. Сообщает о попытке НСД на средства сетевого мониторинга. Имеет возможность загрузки свежих сигнатур хакерских атак с сервера. Выявляет источник атаки сети.
Intruder Alert (инструментарий детектирования сетевых атак)	Alert Technologies	Выбирает стратегию защиты сети. Поддерживает высокий уровень набора правил сетевой защиты. Загружает сигнатуры хакерских атак. Требует наличия опытных специалистов для обслуживания.
Centrax (инструментарий детектирования сетевых атак)	Cyber Safe	Контролирует систему безопасности сети. Осуществляет мониторинг трафика. Выдает предупреждающие сообщения о сетевой атаке. Требует наличия опытных специалистов для обслуживания.
eTrust Intrusion Detection (анализатор трафика сети сегмента)	Computer Associates	Управляет стратегиями защиты. Выдает предупреждения об атаке в режиме реального времени. Осуществляет мониторинг трафика. Предупреждает администратора о нарушениях стратегии защиты. Сообщает о наличии ненормативной лексики в электронной почте. Располагает информацией о злоумышленнике.

Предупреждения, генерируемые агентами BlackICE, очень конкретны. Текст сообщений не заставит администратора усомниться в характере зарегистрированного события, а в большинстве случаев и в его важности. Кроме того, продукт позволяет администратору настроить содержание собственных предупреждающих сообщений, но по большому счету в этом нет необходимости.

Весьма полезным свойством разработок Network ICE, а также пакета Intruder Alert является возможность загрузки самых свежих сигнатур хакерских атак с сервера.

Попытки вывести из строя корпоративный сервер, который в результате вынужден на запросы об обслуживании отвечать отказом (denial-of-service), таят в себе довольно серьезную угрозу бизнесу компаний, предоставляющих своим клиентам услуги по глобальной сети. Суть нападения сводится к тому, что злоумышленник генерирует тысячи запросов SYN (на установление соединения), адресованных атакуемому серверу. Каждый запрос снабжается фальшивым адресом источника, что значительно затрудняет точную идентификацию самого факта атаки и выслеживание атакующего. Приняв очередной запрос SYN, сервер предполагает, что речь идет о начале нового сеанса связи и переходит в режим ожидания передачи данных. Несмотря на то, что данные после этого не поступают, сервер обязан выждать определенное время (максимум 45 с), перед тем как разорвать соединение. Если несколько тысяч таких ложных

запросов будут направлены на сервер в течение считанных минут, он окажется перегружен, так что на обработку настоящих запросов о предоставлении того или иного сервиса ресурсов попросту не останется. Другими словами, в результате SYN-атаки настоящим пользователям будет отказано в обслуживании.

Во всех описываемых системах, за исключением eTrust Intrusion Detection корпорации Computer Associates, использована модель программных агентов, которые сначала инсталлируются на сетевых устройствах, а затем осуществляют сбор информации о потенциальных атаках и пересылают ее на консоль. Агенты выявляют случаи нарушения установленных стратегий защиты и после этого генерируют соответствующие сообщения.

Системы на базе агентов являются наилучшим решением для коммутируемых сетей, поскольку в таких сетях не существует какой-либо одной точки, через которую обязательно проходит весь трафик. Вместо того чтобы следить за единственным соединением, агент осуществляет мониторинг всех пакетов, принимаемых или отправляемых устройством, где он установлен. В результате злоумышленникам не удается «отсидеться» за коммутатором.

Сказанное можно проиллюстрировать на примере продукции фирмы Network ICE. Программе BlackICE отведена роль агента, устанавливаемого в полностью автономной операционной среде, например, на компьютере удаленного пользователя либо на одном из узлов корпоративной сети передачи данных. Обнаружив хакера, атакующего удаленную машину, агент выдаст предупреждение непосредственно на ее экран. Если же аналогичное событие окажется зафиксировано в корпоративной сети, сообщение о попытке несанкционированного доступа будет передано другому приложению — ICEcap, содержащему средства сетевого мониторинга. Последнее собирает и сопоставляет информацию, поступающую от разных подчиненных ему агентов, и это дает ему возможность оперативно выявлять события, действительно угрожающие безопасности сети.

Система eTrust, напротив, основана на централизованной архитектуре. Она устанавливается на центральном узле и анализирует трафик в подведомственном сетевом сегменте. Отсутствие агентов не позволяет данному продукту отслеживать все события в коммутируемой сети, поскольку в ней невозможно выбрать единственную «смотровую площадку», откуда вся сеть была бы видна как на ладони.

Пакет Intruder Alert и система Centrax производства CyberSafe представляют собой скорее инструментарий для построения собственной системы детектирования сетевых атак. Чтобы в полной мере воспользоваться их возможностями, организация должна иметь в своем штате программистов соответствующей квалификации либо располагать бюджетом, позволяющим заказать подобную работу.

Несмотря на то, что все описываемые продукты легко инсталлировать, управление системами Intruder Alert и Centrax простым не назовешь. Скажем, если Centrax выдает предупреждающее сообщение неизвестного или неопределенного содержания (а такая ситуация не раз имела место в наших тестах), администратор вряд ли сумеет быстро определить, что же, собственно, произошло, особенно если для уточнения диагноза ему придется обратиться к файлам регистрации событий. Эти файлы отличаются исчерпывающей полнотой, однако разработчики, по-видимому, решили, что обычному человеку достаточно только намекнуть, о чем может идти речь, и характер про-

исходящего будет безошибочно идентифицирован. В регистрационных журналах этой системы присутствуют описания выданных предупреждений, но нет их идентификаторов. Администратор видит адреса портов, к которым относились подозрительные запросы, либо параметры других операций, но не получает никакой информации о том, что же все это может означать.

Отмеченное обстоятельство значительно снижает ценность сообщений, выдаваемых в режиме реального времени, поскольку невозможно сразу сообразить, отражает ли описание события реальную угрозу системе безопасности или это всего лишь попытка провести более тщательный анализ трафика. Иными словами, покупать названные продукты имеет смысл лишь в том случае, если в штате вашей организации есть опытные специалисты по информационной безопасности.

Программное обеспечение eTrust Intrusion Detection корпорации Computer Associates представляет собой нечто большее, чем просто систему мониторинга сетевой активности и выявления хакерских атак. Этот продукт способен не только декодировать пакеты различных протоколов и служебный трафик, но и перехватывать их для последующего вывода на управляющую консоль в исходном формате. Система осуществляет мониторинг всего трафика TCP/IP и предупреждает администратора о случаях нарушения установленных стратегий в области информационной безопасности. Правда, эта разработка не поддерживает такого же уровня детализации наборов правил, как Intruder Alert.

Однако детектирование попыток несанкционированного доступа и выдача предупреждающих сообщений — это только полдела. Программные средства сетевой защиты должны остановить действия хакера и принять контрмеры. В этом смысле наилучшее впечатление производят пакеты Intruder Alert и Centrax, те самые, что вызвали немалые нарекания по части настройки конфигурации. Если программы фирмы Network ICE и ПО eTrust мгновенно закрывают угрожающие сеансы связи, то системы Intruder Alert и Centrax идут еще дальше. Например, приложение компании Axent Technologies можно настроить таким образом, что оно будет запускать тот или иной командный файл в зависимости от характера зарегистрированных событий, скажем перезагружать сервер, который подвергся атаке, приводящей к отказу в обслуживании.

Отразив атаку, хочется сразу перейти в контрнаступление. Приложения Black-ICE и Centrax поддерживают таблицы с идентификаторами хакеров. Эти таблицы заполняются после прослеживания всего пути до «логовища», где затаился неприятель. Возможности программного обеспечения BlackICE особенно впечатляют, когда дело доходит до выявления источника атаки, расположенного внутри или вне сети: несмотря на многочисленные хитроумные маневры, нам так и не удалось сохранить инкогнито.

А вот система eTrust поражает степенью проникновения в характер деятельности каждого пользователя сети, зачастую даже не подозревающего о том, что он находится под пристальным наблюдением. Одновременно этот пакет предоставляет наиболее полную (и, пожалуй, наиболее точную) информацию о злоумышленниках, даже о том, где они находятся.

Приложение Centrax способно создавать так называемые файлы-приманки, присваивая второстепенному файлу многозначительное название вроде «Ведо-МосТь.xls» и тем самым вводя в заблуждение излишне любопытных пользователей. Такой алгоритм представляется нам слишком прямолинейным, но и он может сослужить непло-

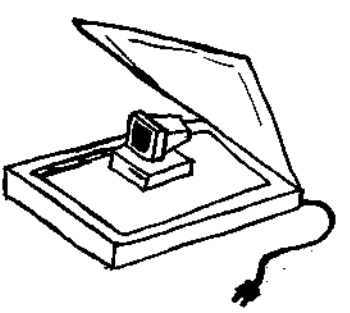
хую службу: с его помощью удается «застукать» сотрудников за «прочесыванием» корпоративной сети на предмет выявления конфиденциальной информации.

Каждый из рассмотренных программных продуктов генерирует отчеты о подозрительных случаях сетевой активности. Высоким качеством таких отчетов и удобством работы с ними выделяются приложения ICEcap и eTrust Intrusion Detection. Последний пакет отличается особенной гибкостью, возможно, потому, что ведет свое происхождение от декодера протоколов. В частности, администратор может проанализировать сетевые события в проекции на отдельные ресурсы, будьте протоколы, станции-клиенты или серверы. В eTrust предусмотрено множество заранее разработанных форматов отчетов. Их хорошо продуманная структура заметно облегчает обнаружение злоумышленников и позволяет наказать провинившихся пользователей.

Каждый продукт имеет свои сильные и слабые стороны, поэтому рекомендовать его можно только для решения определенных задач. Если речь идет о защите коммутируемых сетей, неплохим выбором являются разработки Network ICE, Axent Technologies и CyberSafe. Пакет eTrust Intrusion Detection идеален для своевременного уведомления о случаях нарушения этики бизнеса, например, об употреблении ненормативной лексики в сообщениях электронной почты. Системы Intruder Alert и Centrax — прекрасный инструментарий для консультантов по вопросам информационной безопасности и организаций, располагающих штатом профессионалов в данной области. Однако тем компаниям, которые не могут себе позволить прибегнуть к услугам высокооплачиваемых специалистов, рекомендуем установить продукты компании Network ICE. Эти приложения заменят истинного эксперта по сетевой защите лучше любой другой системы из тех, что когда-либо попадалась нам на глаза.

Сканеры как средства проверки защиты сети

Когда-то давным-давно (или не очень) жесткие диски персональных компьютеров были объемом всего-навсего 10 Мбайт, а их оперативная память не превышала 640 Кбайт. Модемы работали на скоростях от 300 до 1200 бит/с, и мало кто из пользователей слышал о глобальной компьютерной сети Internet. Конечно, эта сеть существовала уже тогда, но использовалась исключительно в военных целях, а работать с ней можно было только при помощи командной строки. Но не это служило основным препятствием для массового доступа к сети Internet. Вычислительные машины, которые могли быть задействованы в качестве серверов, были очень дорогими — их стоимость исчислялась миллионами долларов. Да и сами персональные компьютеры стоили тогда весьма недешево, и были по карману только обеспеченным людям.



Но уже тогда находились люди, которые охотились за чужими секретами. Представим себе, как за персональным компьютером сидит юноша лет 15—17 и обзванивает при помощи модема телефонные номера, которые ему сообщил приятель. В большинстве случаев на другом конце провода оказывается другой модем, и на экране монитора появляется приглашение зарегистрироваться, т. е. ввести имя и пароль.

Каждый раз, получив такое регистрационное приглашение, юноша начинает лихорадочно перебирать различные пары имен и соответствующих им паролей. Наконец, одна пара подходит, и юный взломщик получает возможность управлять удаленным компьютером, не выходя из дома.

Сейчас уже трудно поверить, что первым компьютерным взломщикам приходилось так напрягаться. Ведь известно, что они очень не любят выполнять рутинную работу и при всяком удобном случае стараются заставить свои компьютеры заниматься такой работой. Поэтому неудивительно, что компьютерные взломщики вскоре создали специальное программное средство, чтобы не набирать вручную дюжину команд. Это программное средство назвали боевым номеронабирателем.

Боевой номеронабиратель представляет собой программу, обзванивающую заданные пользователем телефонные номера в поисках компьютеров, которые в ответ на поступивший звонок выдают регистрационное приглашение. Программа аккуратно сохраняет в файле на жестком диске все такие телефонные номера вместе с данными о скорости соединения с ними. Один из самых известных и совершенных боевых номеронабирателей — TONELOC, предназначенный для работы в среде операционной системы DOS (он может быть запущен под управлением Windows 95/98 в режиме командной строки).

Дальнейшее совершенствование боевых номеронабирателей привело к созданию сканеров. Первые сканеры были весьма примитивными и отличались от боевых номеронабирателей только тем, что специализировались исключительно на выявлении компьютеров, подключенных к сети Internet или к другим сетям, использующим протокол TCP/IP. Они были написаны на языке сценариев программной оболочки операционной системы UNIX. Такие сканеры пытались подсоединиться к удаленной хост-машине через различные порты TCP/IP, отправляя всю информацию, которая выводилась на устройство стандартного вывода этой хост-машины, на экран монитора того компьютера, где был запущен сканер.

Ныне сканеры стали грозным оружием как нападения, так и защиты в Internet. Что же представляет собой современный сканер?

Сканер — это программа, предназначенная для автоматизации процесса поиска слабостей в защите компьютеров, подключенных к сети в соответствии с протоколом TCP/IP. Наиболее совершенные сканеры обращаются к портам TCP/IP удаленного компьютера и в деталях протоколируют отклик, который они получают от этого компьютера. Запустив сканер на своем компьютере, пользователь, даже не выходя из дома, может найти бреши в защитных механизмах сервера, расположенного, например, на другом конце земного шара.

Большинство сканеров предназначено для работы в среде UNIX, хотя к настоящему времени такие программы имеются практически для любой операционной системы. Возможность запустить сканер на конкретном компьютере зависит от операционной системы, под управлением которой работает этот компьютер, и от параметров подключения к Internet. Есть сканеры, которые функционируют только в среде UNIX, а с остальными операционными системами оказываются несовместимыми. Другие отказываются нормально работать на устаревших компьютерах с Windows 3.11 и с медленным (до 14 400 бит/с) доступом по коммутируемым линиям к Internet. Такие компьютеры будут надоедать сообщениями о переполнении стека, нарушении прав доступа или станут просто зависать.

Критичным является и объем оперативной памяти компьютера. Сканеры, которые управляются при помощи командной строки, как правило, предъявляют более слабые требования к объему оперативной памяти. А самые «прожорливые» — сканеры, снабженные оконным графическим интерфейсом пользователя.

Написать сканер не очень трудно. Для этого достаточно хорошо знать протоколы TCP/IP, уметь программировать на C или Perl и на языке сценариев, а также разбираться в программном обеспечении сокетов. Но и в этом случае не следует ожидать, что созданный вами сканер принесет большую прибыль, поскольку в настоящее время предложение на рынке сканеров значительно превышает спрос на них. Поэтому наибольшая отдача от усилий, вложенных в написание сканера, будет скорее моральной (от осознания хорошо выполненной работы), чем материальной.

Не стоит переоценивать положительные результаты, которых можно достичь благодаря использованию сканера. Действительно, сканер может помочь выявить дыры в защите хост-машины, однако в большинстве случаев информацию о наличии этих дыр сканер выдает в завуалированном виде, и ее надо еще уметь правильно интерпретировать. Сканеры редко снабжают достаточно полными руководствами пользователя. Кроме того, сканеры не в состоянии сгенерировать пошаговый сценарий взлома компьютерной системы. Поэтому для эффективного использования сканеров на практике прежде всего необходимо научиться правильно интерпретировать собранные с их помощью данные, а это возможно только при наличии глубоких знаний в области сетевой безопасности и богатого опыта.

Обычно сканеры создают и применяют специалисты в области сетевой безопасности. Как правило, они распространяются через сеть Internet, чтобы с их помощью системные администраторы могли проверять компьютерные сети на предмет наличия в них изъянов. Поэтому обладание сканерами, равно как и их использование на практике, вполне законно. Однако рядовые пользователи (не системные администраторы) должны быть готовы к тому, что, если они будут применять сканеры для обследования чужих сетей, то могут встретить яростное сопротивление со стороны администраторов этих сетей.

Более того, некоторые сканеры в процессе поиска брешей в защите компьютерных сетей предпринимают такие действия, которые по закону можно квалифицировать как несанкционированный доступ к компьютерной информации, или как создание, использование и распространение вредоносных программ, или как нарушение правил эксплуатации компьютеров, компьютерных систем и сетей. И если следствием этих деяний стало уничтожение, блокирование, модификация или копирование информации, хранящейся в электронном виде, то виновные лица в соответствии с российским законодательством подлежат уголовному преследованию. А значит, прежде чем начать пользоваться первым попавшимся под руку бесплатным сканером для UNIX-платформ, стоит убедиться, а не копирует ли случайно этот сканер заодно и какие-нибудь файлы с диска тестируемой им хост-машины (например, файл password из каталога /ETC).

Часто к сканерам ошибочно относят утилиты типа host, rusers, finger, Traceroute, Showmount. Связано это с тем, что, как и сканеры, данные утилиты позволяют собирать полезную статистическую информацию о сетевых службах на удаленном компьютере. Эту информацию можно затем проанализировать на предмет выявления ошибок в их конфигурации.

Действительно, сетевые утилиты выполняют ряд функций, которые характерны для сканеров. Однако в отличие от них использование этих утилит вызывает меньше подозрений у системных администраторов. Выполнение большинства сетевых утилит на удаленной хост-машине практически не оказывает никакого влияния на ее функционирование. Сканеры же зачастую ведут себя как слон в посудной лавке и оставляют следы, которые трудно не заметить. Кроме того, хороший сканер — явление довольно редкое, а сетевые утилиты всегда под рукой. К недостаткам сетевых утилит можно отнести то, что приходится выполнять вручную слишком большую работу, чтобы добиться того же результата, который при помощи сканера получается автоматически.

Методы и средства защиты информации от НСД

Проблему безопасности компьютеров и компьютерных сетей надуманной назвать никак нельзя. Как показывает практика, чем больше и масштабнее сеть и чем более ценная информация доверяется подключенным к ней компьютерам, тем больше находится желающих нарушить ее нормальное функционирование ради материальной выгоды, просто по незнанию или из праздного любопытства. Эти атаки не знают государственных границ. В Internet — самой крупной компьютерной сети в мире -, впрочем как и в любой другой, идет постоянная виртуальная война, в ходе которой организованности системных администраторов противостоит изобретательность компьютерных взломщиков. Атаки на компьютерные системы возникают подобно волнам цунами и сметают все защитные барьеры, очень часто оставляя после себя только впавшие в паралич компьютеры, зависшие серверы или опустошенные винчестеры.

Стандартность архитектурных принципов построения, оборудования и программного обеспечения персональных компьютеров, высокая мобильность программного обеспечения и ряд других признаков определяют сравнительно легкий доступ профессионала к информации, находящейся в персональном компьютере.

Особенности защиты персональных компьютеров обусловлены спецификой их использования. Как правило, компьютером пользуется ограниченное число пользователей. Компьютеры могут работать как в автономном режиме, так и в составе локальных сетей (сопряженными с другими компьютерами), подключаясь к удаленному компьютеру или локальной сети с помощью модема по линии связи.

Если персональным компьютером пользуется группа пользователей, то может возникнуть необходимость в разграничении их доступа к информации, особенно если на нем обрабатывается конфиденциальная, а тем более секретная информация.

Любая информация, которая функционирует в компьютерах и компьютерных сетях, содержит определенное смысловое содержание и прикреплена к конкретному носителю: файлу, полю базы данных, данные любого программного приложения. Очевидно, что носителем информации являются также каталог, жесткий диск персонального компьютера или сервера, на котором хранится файл, база данных и т. п. При передаче информации от одного объекта другому носителем информации на какое-то время становится канал ее передачи. Также следует учитывать, что защиты требует не только сама информация, но и среда ее обработки, то есть программное обеспечение.

Несанкционированный доступ к информации — это незапланированное ознакомление, обработка, копирование, применение различных вирусов, в том числе разрушающих программные продукты, а также модификация или уничтожение информации в нарушение установленных правил разграничения доступа.

Поэтому, в свою очередь, защита информации от несанкционированного доступа призвана не допустить злоумышленника к носителю информации. В защите информации компьютеров и сетей от НСД можно выделить три основных направления:

- О ориентируется на недопущение нарушителя к вычислительной среде и основывается на специальных технических средствах опознавания пользователя;
- ❑ связано с защитой вычислительной среды и основывается на создании специального программного обеспечения;
- ❑ связано с использованием специальных средств защиты информации компьютеров от несанкционированного доступа.

Следует иметь в виду, что для решения каждой из задач применяются как различные технологии, так и различные средства. Требования к средствам защиты, их характеристики, функции ими выполняемые и их классификация, а также термины и определения по защите от несанкционированного доступа приведены в руководящих документах Государственной технической комиссии:

- ❑ «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация АС и требования по защите информации»;
- О «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации»;
- ❑ «Зашита от несанкционированного доступа к информации. Термины и определения».

Технические средства, реализующие функции защиты можно разделить на:

Рис. 3.12. Технические средства защиты информации от НСД

- встроенные;
- внешние.

К встроенным средствам защиты персонального компьютера и программного обеспечения (рис. 3.12) относятся средства парольной защиты BIOS, операционной системы, СУБД. Данные средства могут быть откровенно слабыми — BIOS с паролем супервизора, парольная защита Win95/98, но могут быть и значительно более стойкими — BIOS без паролей супервизора, парольная защита Windows NT, СУБД ORACLE. Использование сильных сторон этих средств позволяет значительно усилить систему защиты информации от НСД.

Внешние средства призваны подменить встроенные средства с целью усиления защиты, либо дополнить их недостающими функциями.

К ним можно отнести:

- аппаратные средства доверенной загрузки;
- аппаратно-программные комплексы разделения полномочий пользователей на доступ;
- средства усиленной аутентификации сетевых соединений.

Аппаратные средства доверенной загрузки представляют собой изделия, иногда называемые «электронным замком», чьи функции заключаются в надежной идентификации пользователя, а также в проверке целостности программного обеспечения компьютера. Обычно это плата расширения персонального компьютера, с необходимым программным обеспечением, записанным либо во Flash-память платы, либо на жесткий диск компьютера.

Принцип их действия простой. В процессе загрузки стартует BIOS и платы защиты от НСД. Он запрашивает идентификатор пользователя и сравнивает его с хранимым во Flash-памяти карты. Идентификатор дополнительно можно защищать паролем. Затем стартует встроенная операционная система платы или компьютера (чаще всего это вариант MS-DOS), после чего стартует программа проверки целостности программного обеспечения. Как правило, проверяются системные области загрузочного диска, загрузочные файлы и файлы, задаваемые самим пользователем для проверки. Проверка осуществляется либо на основе имитовставки алгоритма ГОСТ 28147-89, либо на основе функции хэширования алгоритма ГОСТ Р 34.11-34 или иного алгоритма. Результат проверки сравнивается с хранимым во Flash-памяти карты. Если в результате сравнения при проверке идентификатора или целостности системы выявится различие с эталоном, то плата заблокирует дальнейшую работу, и выдаст соответствующее сообщение на экран. Если проверки дали положительный результат, то плата передает управление персональному компьютеру для дальнейшей загрузки операционной системы.

Все процессы идентификации и проверки целостности фиксируются в журнале. Достоинства устройств данного класса — их высокая надежность, простота и невысокая цена. При отсутствии многопользовательской работы на компьютере функций защиты данного средства обычно достаточно.

Аппаратно-программные комплексы разделения полномочий на доступ используются в случае работы нескольких пользователей на одном компьютере, если встает задача разделения их полномочий на доступ к данным друг друга. Решение данной задачи основано на:

- запрете пользователям запусков определенных приложений и процессов;
- разрешении пользователям и запускаемым ими приложениям лишь определенного типа действия с данными.

Реализация запретов и разрешений достигается различными способами. Как правило, в процессе старта операционной системы запускается и программа защиты от несанкционированного доступа. Она присутствует в памяти компьютера, как резидентный модуль и контролирует действия пользователей на запуск приложений и обращения к данным. Все действия пользователей фиксируются в журнале, который доступен только администратору безопасности. Под средствами этого класса обычно и понимают средства защиты от несанкционированного доступа. Они представляют собой аппаратно-программные комплексы, состоящие из аппаратной части — платы доверенной загрузки компьютера, которая проверяет теперь дополнительно и целостность программного обеспечения самой системы защиты от НСД на жестком диске, и программной части — программы администратора, резидентного модуля. Эти программы располагаются в специальном каталоге и доступны лишь администратору. Данные системы можно использовать и в однопользовательской системе для ограничения пользователя по установке и запуску программ, которые ему не нужны в работе.

Средства усиленной аутентификации сетевых соединений применяются в том случае, когда работа рабочих станций в составе сети накладывает требования для защиты ресурсов рабочей станции от угрозы несанкционированного проникновения на рабочую станцию со стороны сети и изменения либо информации, либо программного обеспечения, а также запуска несанкционированного процесса. Защита от НСД со стороны сети достигается средствами усиленной аутентификации сетевых соединений. Эта технология получила название технологии виртуальных частных сетей.

Одна из основных задач защиты от несанкционированного доступа — обеспечение надежной идентификации пользователя (рис. 3.13) и возможности проверки подлинности любого пользователя сети, которого можно однозначно идентифицировать по тому, что он:

- знает;
- имеет;
- из себя представляет.

Что знает пользователь? Свое имя и пароль. На этих знаниях основаны схемы парольной идентификации. Недостаток этих схем — ему необходимо запоминать сложные пароли, чего очень часто не происходит: либо пароль выбирают слабым, либо его

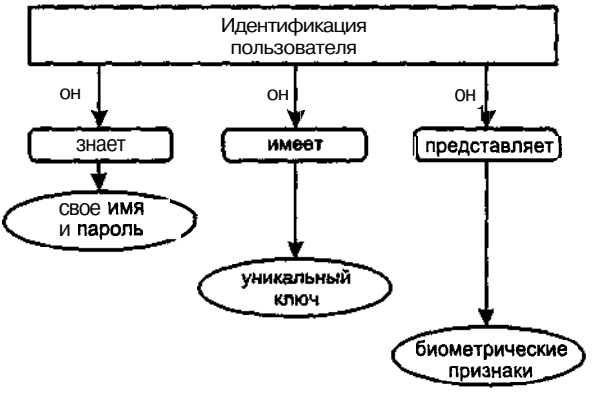


Рис. 3.13. Признаки идентификации пользователя в сети

просто записывают в записную книжку, на листок бумаги и т. п. В случае использования только парольной защиты принимают надлежащие меры для обеспечения управлением создания паролей, их хранением, для слежения за истечением срока их использования и своевременного удаления. С помощью криптографического закрытия паролей можно в значительной степени решить эту проблему и затруднить злоумышленнику преодоление механизма аутентификации.

Что может иметь пользователь? Конечно же, специальный ключ — уникальный идентификатор, такой, например, как таблетка touch memory (I-button), e-token, смарт-карта, или криптографический ключ, на котором зашифрована его запись в базе данных пользователей. Такая система наиболее стойкая, однако требует, чтобы у пользователя постоянно был при себе идентификатор, который чаще всего присоединяют к брелку с ключами и либо часто забывают дома, либо теряют. Будет правильно, если утром администратор выдаст идентификаторы и запишет об этом в журнале и примет их обратно на хранение вечером, опять же сделав запись в журнале.

Что же представляет собой пользователь? Это те признаки, которые присущи только этому пользователю, только ему, обеспечивающие биометрическую идентификацию. Идентификатором может быть отпечаток пальца, рисунок радужной оболочки глаз, отпечаток ладони и т. п. В настоящее время — это наиболее перспективное направление развития средств идентификации. Они надежны и в то же время не требуют от пользователя дополнительного знания чего-либо или постоянного владения чем-либо. С развитием технологи и стоимость этих средств становится доступной каждой организации.

Гарантированная проверка личности пользователя является задачей различных механизмов идентификации и аутентификации.

Каждому пользователю (группе пользователей) сети назначается определенный отличительный признак — идентификатор и он сравнивается с утвержденным перечнем. Однако только заявленный идентификатор в сети не может обеспечить защиту от несанкционированного подключения без проверки личности пользователя.

Процесс проверки личности пользователя получил название — аутентификации. Он происходит с помощью предъявляемого пользователем особого отличительного признака — аутентификатора, присущего именно ему. Эффективность аутентификации определяется, прежде всего, отличительными особенностями каждого пользователя.

Конкретные механизмы идентификации и аутентификации в сети могут быть реализованы на основе следующих средств и процедур защиты информации:

- ❑ пароли;
- ❑ технические средства;
- G средства биометрии;
- ❑ криптография с уникальными ключами для каждого пользователя.

Вопрос о применимости того или иного средства решается в зависимости от выявленных угроз, технических характеристик защищаемого объекта. Нельзя однозначно утверждать, что применение аппаратного средства, использующего криптографию, придаст системе большую надежность, чем использование программного.

Анализ защищенности информационного объекта и выявление угроз его безопасности — крайне сложная процедура. Не менее сложная процедура — выбор технологий и средств защиты для ликвидации выявленных угроз. Решение данных задач лучше поручить специалистам, имеющим богатый опыт.

Парольная защита операционных систем

Контроль доступа, основанный на обладании специфической информацией, наиболее распространен. Он характеризуется тем, что правом доступа обладают лишь те, кто способен продемонстрировать знание определенного секрета, обычно пароля. Это самый простой и дешевый метод защиты любой компьютерной системы. Поскольку его использование не требует больших затрат времени, сил и места в памяти компьютера, то он применяется даже в тех компьютерах, которые вовсе не нуждаются в средствах защиты. Кроме того, владение паролем дает пользователю ощущение психологического комфорта. Более того, это широко используется в системах, уже защищенных другими средствами — магнитными картами или иными программными средствами, типа шифрования, что в еще большей степени повышает уровень защиты от несанкционированного доступа.

До настоящего времени единственным средством защиты компьютерной сети от несанкционированного доступа была парольная система. При стандартной процедуре входа в сеть каждый пользователь должен знать свое сетевое имя и сетевой пароль. Администратор, назначающий эти атрибуты, как правило, не применяет случайных или плохо запоминаемых последовательностей символов, поскольку это может привести к тому, что сетевое имя и пароль могут быть записаны на какой-либо носитель (бумагу, дискету и т. п.), что может привести к утечке секретного пароля и имени пользователя.

Пароли, как правило, рассматриваются в качестве ключей для входа в систему, но они используются и для других целей: блокирование записи на дисковод, в командах на шифрование данных, то есть во всех тех случаях, когда требуется твердая уверенность, что так действовать будут только законные владельцы или пользователи программного обеспечения.

И по сей день во многих случаях для злоумышленника основным (иногда единственным) защитным рубежом против атак в компьютерной сети остается система парольной защиты, которая есть во всех современных операционных системах. В соответствии с установившейся практикой перед началом сеанса работы с операционной системой пользователь обязан зарегистрироваться, сообщив ей свое имя и пароль. Имя нужно операционной системе для идентификации пользователя, а пароль служит подтверждением правильности произведенной идентификации. Информация, введенная пользователем в диалоговом режиме, сравнивается с той, которая имеется в распоряжении операционной системы. Если проверка дает положительный результат, то пользователю будут доступны все ресурсы операционной системы, связанные с его именем.

Трудно представить, что сегодня какому-нибудь злоумышленнику может прийти в голову шальная мысль о том, чтобы попытаться подобрать имя и пароль для входа в операционную систему, по очереди перебирая в уме, все возможные варианты и вводя их с клавиатуры. Скорость такого подбора пароля будет чрезвычайно низкой, тем более, что

в операционных системах с хорошо продуманной парольной защитой количество подряд идущих повторных вводов конкретного пользовательского имени и соответствующего ему пароля всегда можно ограничить двумя-тремя и сделать так, что если это число будет превышено, то вход в систему с использованием данного имени блокируется в течение фиксированного периода времени или до прихода системного администратора.

Поэтому чаще используют более опасный и гораздо более эффективный метод взлома парольной защиты операционной системы, при использовании которого атаке подвергается системный файл, содержащий информацию о ее легальных пользователях и их паролях.

Однако любая современная операционная система надежно *защищает* пользовательские пароли, которые хранятся в этом файле при помощи шифрования. Доступ к таким файлам по умолчанию запрещен, как правило, даже для системных администраторов, не говоря уже о рядовых пользователях. Иногда злоумышленнику удается путем различных ухищрений получить в свое распоряжение файл с именами пользователей и их зашифрованными паролями. И тогда ему на помощь приходят специализированные программы — парольные взломщики, которые и служат для взлома паролей операционных систем. Как же действуют эти программы?

Криптографические алгоритмы, применяемые для шифрования паролей пользователей в современных операционных системах, в подавляющем большинстве случаев слишком стойкие для того, чтобы можно было надеяться отыскать методы их дешифровки, которые окажутся более эффективными, чем тривиальный перебор возможных вариантов. Поэтому парольные взломщики иногда просто шифруют все пароли с использованием того же самого криптографического алгоритма, который применяется для их засекречивания в атакуемой операционной системе, и сравнивают результаты шифрования с тем, что записано в системном файле, где находятся шифрованные пароли ее пользователей. При этом в качестве вариантов паролей парольные взломщики используют символьные последовательности, автоматически генерируемые из некоторого набора символов. Данным способом можно взломать все пароли, если известно их представление в зашифрованном виде и они содержат только символы из этого набора. Максимальное время, требуемое для взлома пароля, зависит от числа символов в наборе, предельной длины пароля и от производительности компьютера, на котором производится взлом ее парольной защиты (зависит от операционной системы и быстродействия).

С увеличением числа символов в исходном наборе, число перебираемых комбинаций растет экспоненциально, поэтому такие атаки парольной защиты операционной системы могут занимать слишком много времени. Однако хорошо известно, что большинство пользователей операционных систем не затрудняют себя выбором стойких паролей (т. е. таких, которые трудно взломать). Поэтому для более эффективного подбора паролей парольные взломщики обычно используют так называемые словари, представляющие собой заранее сформированный список слов, наиболее часто применяемых в качестве паролей.

Для каждого слова из *словаря* парольный взломщик использует одно или несколько *правил*. *В* соответствии с этими правилами слово изменяется и порождает дополнительное множество опробуемых паролей. Производится попеременное изменение

буквенного регистра, в котором набрано слово, порядок следования букв в слове меняется на обратный, в начало и в конец каждого слова приписывается цифра 1, некоторые буквы заменяются на близкие по начертанию цифры (в результате, например, из слова password получается pa55wOrd). Это повышает вероятность подбора пароля, поскольку в современных операционных системах, как правило, различаются пароли, набранные прописными и строчными буквами, а пользователям этих систем настоятельно рекомендуется выбирать пароли, в которых буквы чередуются с цифрами.

Противостоять таким атакам можно лишь в том случае, если использовать стойкие к взлому пароли. Перед тем как ответить на вопрос «Как правильно выбрать пароль?», рассмотрим, какие же пароли используются вообще.

Пароли можно подразделить на семь основных групп:

- пароли, устанавливаемые пользователем;
- пароли, генерируемые системой;
- случайные коды доступа, генерируемые системой;
- полуслова;
- ключевые фразы;
- интерактивные последовательности типа «вопрос-ответ»;
- «строгие» пароли.

Первая группа наиболее распространена. Большинство таких паролей относятся к типу «выбери сам». Для лучшей защиты от несанкционированного доступа необходимо использовать достаточно длинный пароль, поэтому обычно система запрашивает пароль, содержащий не менее четырех-пяти букв. Существуют также и другие меры, не позволяющие пользователю создать неудачный пароль. Например, система может настаивать на том, чтобы пароль включал в себя строчные и прописные буквы вперемешку с цифрами; заведомо очевидные пароли, например, internet, ею отвергаются. В разных операционных системах существует немало программ, которые просматривают файлы, содержащие пароли, анализируют пароли пользователей и определяют, насколько они секретны. Неподходящие пароли заменяются.

Когда человек впервые загружает компьютер, и тот запрашивает у него пароль, этот пароль наверняка окажется вариантом одной из общих и актуальных для всех тем — особенно если у пользователя не хватает времени. Не считая гениев и безнадежных тупиц, все люди, когда надо принимать быстрые решения, мыслят и действуют примерно одинаково. И пользователи выдают первое, что приходит им в голову. А в голову приходит то, что они видят или слышат в данный момент, либо то, что собираются сделать сразу же после загрузки. В результате пароль создается в спешке, а последующая его замена на более надежный происходит достаточно редко. Таким образом, многие пароли, созданные пользователями, можно раскрыть достаточно быстро.

Случайные пароли и коды, устанавливаемые системой, бывают нескольких разновидностей. Системное программное обеспечение может использовать полностью случайную последовательность символов, вплоть до случайного выбора регистров, цифр, пунктуации длины; или же использовать ограничения в генерирующих процедурах. Создаваемые компьютером пароли могут также случайным образом извлекаться из списка обычных или ничего не значащих слов, созданных авторами программы, которые образуют пароли вроде onah.foopn, или ocar-back-treen.

Полуслова частично создаются пользователем, а частично — каким-либо случайным процессом. Это значит, что если даже пользователь придумает легко угадываемый пароль, например, «абзац», компьютер дополнит его какой-нибудь неразберихой, образовав более сложный пароль типа «абзац,3ю37».

Ключевые фразы хороши тем, что они длинные и их трудно угадать, зато легко запомнить. Фразы могут быть осмысленными, типа «мы были обеспокоены этим» или не иметь смысла, например, «ловящий рыбу нос». Следует заметить, что в программировании постепенно намечается тенденция к переходу на более широкое применение ключевых фраз. К концепции ключевых фраз близка концепция кодового акронима, который эксперты по защите оценивают как короткую, но идеально безопасную форму пароля. В акрониме пользователь берет легко запоминающееся предложение, фразу, строчку из стихотворения и т. п., и использует первые буквы каждого слова в качестве пароля. Например, акронимами двух приведенных выше фраз являются «мбоэ» и «лрн». Подобные нововведения в теории паролей значительно затрудняют занятия электронным шпионажем.

Интерактивные последовательности «вопрос- ответ», предлагают пользователю ответить на несколько вопросов, как правило, личного плана: «Девичья фамилия вашей матери?», «Ваш любимый цвет?», и т. д. В компьютере хранятся ответы на множество таких вопросов. При входе пользователя в систему компьютер сравнивает полученные ответы с «правильными». Системы с использованием «вопрос- ответ» склонны прерывать работу пользователя каждые десять минут, предлагая отвечать на вопросы, чтобы подтвердить его право пользоваться системой. В настоящее время такие пароли почти не применяются. Когда их придумали, идея казалась неплохой, но раздражающий фактор прерывания привел к тому, что данный метод практически исчез из обихода.

«Строгие» пароли обычно используются совместно с каким-нибудь внешним электронным или механическим устройством. В этом случае компьютер обычно с простодушным коварством предлагает несколько вариантов приглашений, а пользователь должен дать на них подходящие ответы. Пароли этого типа часто встречаются в системах с одноразовыми кодами.

Одноразовые коды — это пароли, которые срабатывают только один раз. К ним иногда прибегают, создавая временную копию для гостей, чтобы продемонстрировать потенциальным клиентам возможности системы. Они также порой применяются при первом вхождении пользователя в систему. Во время первого сеанса пользователь вводит свой собственный пароль и в дальнейшем входит в систему лишь через него. Одноразовые коды могут также применяться в системе, когда действительный пользователь входит в нее в первый раз; затем вам следует поменять свой пароль на более секретный персональный код. В случаях, когда системой пользуется группа людей, но при этом нельзя нарушать секретность, прибегают к списку одноразовых кодов. Тот или иной пользователь вводит код, соответствующий времени, дате или дню недели.

Итак, для того чтобы пароль был действительно надежен, он должен отвечать определенным требованиям:

- ❑ быть определенной длины;
- ❑ включать в себя прописные и строчные буквы;
- О включать в себя одну и более цифр;
- ❑ включать в себя один нецифровой и один неалфавитный символ.

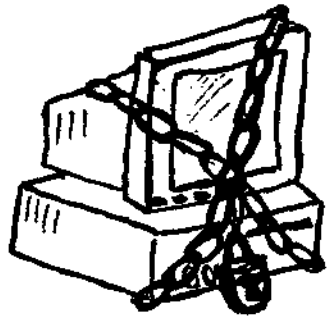
Одно или несколько из этих правил должны обязательно соблюдаться. Необходимо помнить, что пароль — это самая слабая часть любой системы защиты данных, какой бы изощренной и надежной она ни была. Именно поэтому его выбору и хранению надо уделить должное внимание. Не стоит обольщаться и тешиться своей безопасностью при работе с Windows 95/98, если видите, в каком-либо диалоговом окне ваш пароль, скрытый звездочками — это защита «от дурака». С помощью крохотной программы можно посмотреть скрытый звездочками пароль, всего лишь установив курсор мыши на диалоговое окно.

Защита сети от НСД с помощью аппаратно-программных средств

С распространением Internet, электронной коммерции и удаленного доступа появляется все больше разнообразных идентификационных устройств. Положительной стороной данного процесса является то, что эти устройства становятся более доступными по цене, удобными в инсталляции, реализации и простыми в обращении. Это, конечно, прекрасно с точки зрения защиты, но не так уж замечательно с точки зрения администрирования. Изобилие подобных устройств означает, что администратору сети придется «дирижировать» еще большим числом компонентов.

Действенным способом, делающим вход в сеть более корректным (по соображениям защиты от несанкционированного доступа), является возможность избавления пользователя от обязанности запоминания перечисленных выше атрибутов. Имя и пароль могут быть записаны в память специального носителя информации — ключа-идентификатора, в качестве которого применяют, например, интеллектуальные (микропроцессорные) карты или жетоны. В процессе запуска или работы защищаемое программное приложение сверяет этот особый ключ с эталонным. В случае совпадения ключей программа функционирует в заданном режиме, если нет — прекращается выполнение операций в программе.

Несколько лет тому назад в качестве особого ключа защиты использовались некопируемая ключевая дискета или уникальные характеристики компьютера. В настоящее время для этих целей применяют более современные и удобные устройства — электронные ключи, позволяющие решать задачи обеспечения информационной безопасности на любом программно-аппаратном уровне. При этом электронные ключи могут иметь различные характеристики, содержать перезаписываемую энергонезависимую память (EEPROM) и генерировать защитную функцию F(x). Встроенная в программу система защиты получает через ключ информацию, которая используется для аутентификации пользователя и определения набора доступных функции.



Электронные ключи имеют ряд достоинств:

- программа или база данных привязаны не к компьютеру, а к ключу, через который пользователь получает доступ к данным;
- при запуске защищенная программа проверяется на наличие вирусов и несанкционированных изменений;

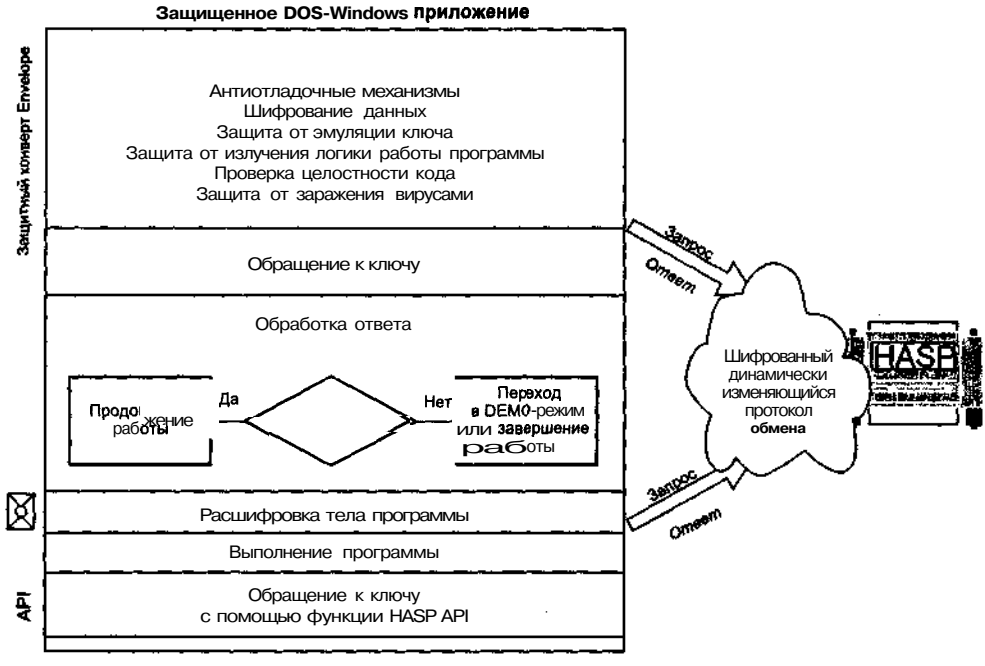


Рис. 3.14. Схема защиты

- в процессе работы пользователи имеют возможность получать новые версии программ при перепрограммировании ключей соответствующими администраторами.

Важнейшей частью системы защиты с использованием электронных ключей является ее программный компонент. Как правило, он включает в себя:

- защитный «конверт» (Envelope);
- библиотечные функции обращения к ключу API (Applications Program Interface).

Каждый из этих способов обеспечения безопасности имеет свое назначение, но в идеале они должны применяться совместно. Системы автоматической защиты (рис. 3.14) предназначены для защиты уже готовых приложений без вмешательства в исходный код программы. Таким образом обеспечивается сохранность COM-, EXE-файлов, библиотеки DLL. Для встраивания дополнительного модуля внутрь используется «вирусная» технология вживления и перехвата на себя управления после загрузки.

При использовании «конверта» тело программы шифруется, в нее встраивается дополнительный модуль, который в момент запуска берет управление на себя. После отработки специальных антиотладочных и антитрассировочных механизмов выполняются следующие действия:

- проверка наличия «своего» электронного ключа и считывание из него требуемых параметров;
- анализ «ключевых» условий и выработка решения.

Для защиты от аппаратной или программной эмуляции обмен между «конвертом» и электронным ключом выполняется с использованием зашумленного изменяющегося во времени («плавающего») протокола.

Некоторые «конверты» обеспечивают фоновые проверки ключа в процессе работы приложения, так что перенести ключ на другой компьютер после того как защищенная программа запущена, невозможно.

Функции API предназначены для выполнения низкоуровневых операций с ключом, простейшая из которых — проверка наличия ключа. Более сложные функции могут посылать ключу различные входные коды и получать от него ответные, которые затем поверяются на соответствие установленным значениям. Они также могут использоваться в каких-либо вычислительных операциях или при декодировании данных. Программа может обращаться к ключу из различных мест, а результаты могут быть разбросаны по телу программы и хорошо замаскированы.

Библиотеки функций API поставляются совместно с электронными ключами HASP (Hardware Adainst Software Piracy) для различных языков программирования, компиляторов и т. п.

В последнее время особую важность приобретает не столько защита кода программного продукта, сколько конфиденциальность содержащихся в нем данных (информационного наполнения).

Для защиты от несанкционированного доступа к программам и данным широко используются криптографические системы защиты. Одна из популярных систем защиты программ и данных — Professional ToolKit компании Aladdin Software Security. Эта система позволяет защищать методом прозрачного шифрования практически любые файлы данных: графические, текстовые, электронные таблицы и т. п. Метод прозрачного шифрования осуществляется в среде Windows *95 с* помощью электронных ключей HASP — алгоритмы кодирования/декодирования IDEA (International Data Encryption Algorithm); длина ключа — 128 бит.

Система не имеет ограничений по количеству открытых файлов и числу приложений, работающих с защищенной информацией. Внутренние процедуры шифрования драйвера используют данные, содержащиеся в памяти ключа HASP (рис. 3.15), поэтому доступ к зашифрованным файлам без него невозможен. Система поддерживает электронные ключи типа MemoHASP, TimeHASP и NetHASP, причем каждый экземпляр системы работает с одной серией ключей.

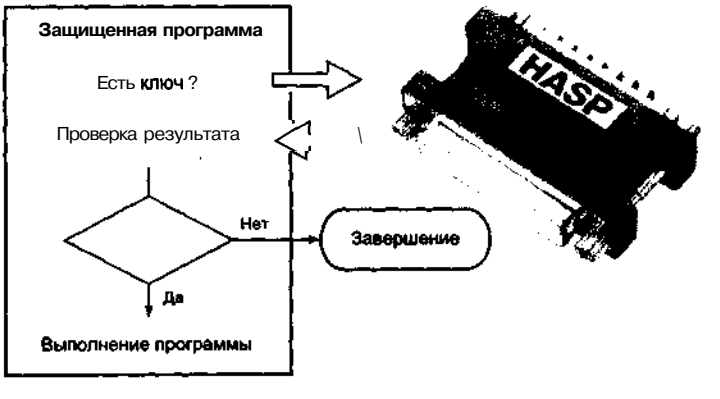


Рис. 3.15. Электронный ключ HASP

«Интеллектуальные» и физические возможности ключа в основном определяются базой на которой он собран. Сердцем ключа HASP является «заказной» ASIC-чип (Application Specific Integrated). Логику его функционирования практически невозможно реализовать с помощью стандартных наборов микросхем.

Ключ HASP позволяет использовать функцию Y = F(X), где X — посылаемое в ключ целое число в диапазоне от 0 до 65 535, а Y — возвращаемые ключом четыре целых числа из того же диапазона, уникальных для каждой серии. Использование механизма генерации чисел качественно усложняет задачу взлома, так как ключевая информация (пароли, шифровальные ключи, часть самого кода и т. п.) не хранится ни в теле программы, ни в памяти ключа ни в открытом, ни в зашифрованном виде. Существует несколько модификаций ключей HASP:

- MemoHASP — ключ с внутренней энергонезависимой памятью до 4 кбит, доступной для чтения и записи; подключается к параллельному порту;
- TimeHASP — содержит встроенные часы с автономным питанием и память до 496 байт; может использоваться для подготовки учебной или демонстрационной версии программы (ограниченный срок работы), для сдачи программы в аренду или в лизинг для периодического сбора абонентской платы;
- MacHASP — микропроцессорные ключи для защиты приложений под Macintosh;
- NetHASP — ключ для защиты сетевых приложений; предотвращает не только нелегальное тиражирование сетевых программ, но и позволяет контролировать и ограничивать количество пользователей, одновременно работающих с защищенной программой в сети;
- HASP-Card — специальная плата, встраиваемая в стандартный слот компьютера, функционирует как дополнительный свободный параллельный порт; к ней может быть подключено несколько ключей HASP или ключей других типов;
- OpenHASP — микропроцессорные ключи с памятью; предназначены для защиты платформонезависимых приложений, функционирующих на рабочих станциях;
- PC-CardASP — модификация ключей HASP для компьютеров типа notebook.

Персональные компьютеры и микропроцессорные смарт-карты (smart-card) до недавнего времени имели не так уж много точек соприкосновения, так как развивались как бы в разных плоскостях. Основными областями применения смарт-карт являются идентификация владельцев мобильных телефонов, банковские операции, электронные кошельки и розничные транзакции. Однако, как ожидается, этот перечень должен пополниться защитой сети и электронной коммерцией. Признаками этой нарождающейся тенденции может служить поддержка смарт-карт в Windows 2000.

Характерная особенность таких карт — встроенный недорогой, но достаточно производительный микропроцессор. В итоге появляются возможности реализации на уровне пластиковой карты оперативных вычислений, обеспечения надлежащего уровня конфиденциальности и сохранности данных в блоках памяти, а также применения аппаратных методов шифрования. На одной и той же карте может быть реализовано сразу несколько ключей (полномочий пользователя) к различным системным или сетевым ресурсам (рис. 3.16), причем в каждом случае речь будет идти о соответствующих персональных идентификационных номерах.

Надежный контроль доступа и операций, совершаемых с различных рабочих мест, — проблема, весьма остро ощущаемая во многих областях и особенно в открытых ком-

пьютерных сетях. В идеале для защиты сетей и успешного и безопасного взаимодействии в рамках открытой сети лучше всего подходит реализация алгоритма шифрования данных с открытым ключом. Такие алгоритмы обеспечивают высокий уровень защиты передаваемых сообщений. При этом не представляет сложности процесс первичной генерации секретных ключей, а кроме того, не нужно ломать голову над тем, как безопасным способом сообщить свой секретный ключ другой стороне. Все участники сетевого общения, принявшие данный стандарт передачи сообщений, имеют возможность использовать его где и когда угодно, не боясь раскрытия каких-либо секретов.

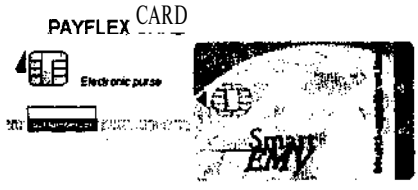


Рис. 3.16. Многоцелевая смарт-карта

В рамках такой технологии смарт-карта может выполнять роль криптопроцессора, генерирующего ключи, и применять самые различные алгоритмы шифрования: DES, «тройной DES», PGP, ГОСТ 28147-89 и т. п.

Среди множества компаний, выпускающих смарт-карты, выделяется RSA Security, чья смарт-карта SecurID 3100 Smart Card поддерживает конфигурации с одним и двумя сертификатами и хранит мандаты пользователя. Карта может хранить два цифровых сертификата и регистрационную информацию о паролях пользователя.

Несмотря на все преимущества смарт-карт, их эффективность резко снижается без необходимого программного обеспечения. Карта SecurID 3100 Smart Card работает с программным обеспечением управления ACE/Server компании RSA. Программное обеспечение служит для проверки и идентификации запросов и администрирования правил.

Пакет ActivCard Gold компании ActivCard включает смарт-карты, клиентское программное обеспечение и, по желанию, считыватель смарт-карт. С помощью этого идентификационного пакета для настольных систем пользователи могут локально зарегистрироваться в домене Windows NT, получить удаленный доступ, войти на корпоративный Web-сервер, а также поставить электронную подпись и зашифровать свою электронную почту.

В зависимости от вида сервиса доступ к нему может контролироваться с помощью фиксированных паролей, динамических паролей или цифровых сертификатов. Как было недавно объявлено, ActivCard Gold совместима с технологией PKI компании Baltimore Technologies.

Сматр-карты GemSAFE Enterprise компании GemPlus представляют собой комплект карт для реализации PKI. Клиенты получают такие возможности, как цифровая подпись на базе смарт-карт, а также шифрование электронной почты и файлов и поддержка хранения сертификатов X.509V3. Административные функции включают удаленную диагностику, управление картами (например, выпуск и аннулирование) и пользователями, генерацию и восстановление ключей, а также составление отчетов. Система предусматривает одноэтапный процесс персонали-зации карт.

Смарт-карта Model 33 PKI компании DataKey поддерживает 2084-разрядные ключи RSA и имеет память емкостью 32 кбайт. Она может использоваться для идентификации в Internet, Extranet и VPN. В карте применяется технология эллиптических кри-

вых компании Certicom, благодаря которой длина ключей и объем вычислений оказываются меньше.

Кроме того, смарт-карты предлагают и другие производители: Cylink (PrivateCard), Spyrus (Rosetta Smart Card), Card Logix (M.O.S.T.), а также CyberMark и Bull Worldwide Information Systems.

На выставке CardTech SecurTech, которая проходила в Чикаго, фирма Publicard представила новую разработку — реализованную на базе смарт-карт систему проверки паролей и идентификаторов пользователей SmartPassky.

В основу новой системы была заложена идея хранения в одном месте (то есть на смарт-карте) всех паролей, секретных URL-адресов и идентификаторов активно работающего в сети пользователя.

Как заявил представитель фирмы, система на базе единственной смарт-карты, защищенной с помощью одного основного ключа, представляет собой компактное и надежное средство доступа, сочетающее эти свойства с простотой использования закладок Web-браузера.

Когда смарт-карта вставляется в подключаемое к персональному компьютеру специальное считывающее устройство, SmartPassky выдает запрос на ввод кода доступа пользователя Internet. После ввода кода перед пользователем отображается заранее сформированный список защищенных URL-адресов. После выбора нужного Web-адреса SmartPassky инициирует процедуру регистрации выбранного узла и автоматически «вводит» идентификатор и пароль пользователя. Для завершения процедуры пользователю остается лишь щелкнуть на соответствующем поле на экране регистрации.

Кроме смарт-карт, в качестве персонального идентификатора в системах ограничения доступа используются электронные ключи-жетоны, поддерживающие контактную или бесконтактную технологию.

Жетоны представлены множеством разновидностей, отличающихся по форме и дизайну. В зависимости от таких факторов, как требования к защите, состав пользователей и потребность в масштабировании, они могут оказаться более предпочтительным решением, чем смарт-карты. Жетоны бывают как аппаратные, так и программные.

К числу производителей жетонов принадлежит компания Secure Computing. Она выпускает устройство в формате для связки ключей SafeWord Silver 2000 и SafeWord Platinum Card. Устройство поддерживает статические и динамические пароли и различные платформы, такие, как Windows NT, Linux, Solaris и HP-UX. Через агентов SafeWord устройства могут также взаимодействовать с Citrix WinFrame и MetaFrame, Internet Information Server (US), NT RAS, Netscape Enterprise Server и доменами NT. Secure Computing имеет также агентов SafeWord для персональных цифровых секретарей Palm и мобильных телефонов компании Ericsson.

Продукт Luna CAз на базе PKI компании Chrysalis-ITS обеспечивает аппаратную защиту основного ключа (root-keyprotection). Генерация, хранение, резервирование, подпись и удаление ключей доверяются сертификационным сервером (Certificate Authority, CA) уполномоченному жетону. Luna Key Cloning производит резервное копирование зашифрованных цифровых ключей с одного жетона на другой, а Luna PED обеспечивает доступ через устройство ввода персонального идентификационного кода PIN (Personal Identification Number).

Программы управления жетонами CryptoAdminобеспечивают централизованную идентификацию и децентрализованное администрирование жетонов.

Продукты Digipass компании Vasco Data Security включают жетоны на базе карт, устройства в стиле калькуляторов и устройство для идентификации с использованием радиопередачи или идентификационных карт для контроля за физическим доступом и входом в сеть.

Сервер контроля доступа Vacman Optimum обеспечивает программирование/перепрограммирование устройств, а также управление кодами PIN. Кроме того, пакет включает Vacman Programmer 1.0, несколько устройств Digipass и Administrator Digipass.

Другой продукт, где используются радиоволны, — VicinID Card компании First Access. Система включает датчики Vicinity Sensor, устанавливаемые на каждой рабочей станции, и программное обеспечение. VicinID Server идентифицирует пользователей, имеющих с собой карту, и предоставляет или запрещает им доступ к конкретной рабочей станции в зависимости от их профиля доступа. Кроме того, продукт поддерживает так называемую непрерывную идентификацию, т. е. постоянно следит за тем, что рабочей станцией пользуются те, кто имеет на это право.

В качестве недорого и эффективного персонального идентификатора в системах ограничения доступа используются электронные жетоны Touch Memory (iButton) — специализированные высоконадежные приборы производстна фирмы Dallas Semiconductor Inc. (США). С начала 1997 года Dallas Semiconductor заявила о смене названия всех своих идентификационных ключей с Touch Memory на iButton (Information Button — Таблетка с информацией), как более общее и охватывающее весь ряд изделий в настоящем и в будущем. Они представляют собой микросхему, размещенную в прочном корпусе из нержавеющей стали, по размерам и форме напоминающем элемент питания от электронных часов (рис. 3.17). Металл представляет собой нержавеющую сталь. Диаметр диска около 17 мм, толщина 3,1 мм или 5,89 мм. Диск состоит из двух электрически разъединенных половинок. Внутри он полый. В герметичную полость заключена электронная схема на кремниевом кристалле. Выход схемы соединен с половинками диска двумя проводниками. Половинки диска образуют контактную часть однопроводного последовательного порта. При этом через центральную часть идет линия данных, внешняя оболочка — земля. Для того чтобы произошел обмен информации iButton с внешними устройствами, необходимо прикоснуться

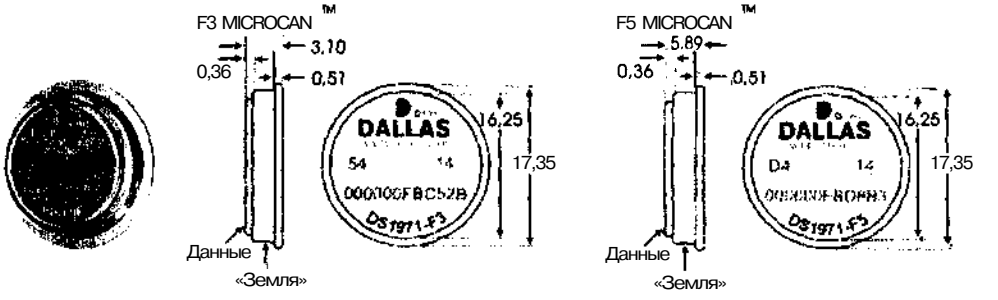


Рис. 3.17. Электронный жетон iButton

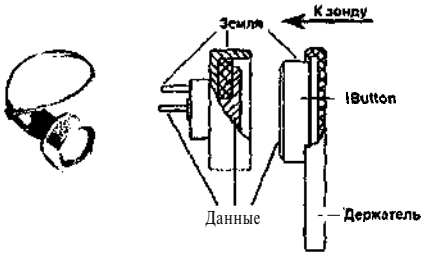


Рис. 3.18. Считыватель электронных жетонов iButton

обеими поверхностями половинок металлического диска к контактному устройству (зонду), также состоящему из двух электрически не связанных, проводящих электрический ток частей.

Большая площадь поверхности контактов защищает систему от неточного совмещения при подключении по причине «человеческого фактора» или при автоматизированном касании, когда идентификатор и зонд расположены на различных подвижных механизмах. Кроме того, дисковая форма корпуса направляет и очищает контакты, гарантируя надежное соединения, а закругленный край корпуса легко совмещается с зондом. Считыватель электронных жетонов iButton представлен на рис. 3.18.

Вход на рабочие станции и локальные вычислительные сети осуществляется при касании считывающего устройства зарегистрированной электронной карточкой Touch Memory и вводом с нее пароля и имени пользователя. В памяти Touch Memory (iButton), применяющейся для входа в сеть, записано 64 символа сетевого имени и 64 символа сетевого пароля. Эти значения генерируются датчиком псевдослучайных чисел, зашифровываются и записываются в iButton, оставаясь неизвестными даже пользователю. Корректность выполнения процедуры регистрации пользователя в сети обеспечивается передачей управления стандартным сетевым средствам после аутентификации пользователя. Кроме применения электронной карты, для более жесткого контроля входа в сеть пользователь вводит личный секретный пароль. Изделие этого ряда DS1954 имеет внутри своего корпуса специальный микропроцессор для шифрования информации.

Модель DS1957B iButton имеет память, которой достаточно для хранения всех данных о личности владельца. Она работает и как обычный дверной ключ, который прикладывается к двери и открывает электронный замок, и как компьютерный ключ для входа в защищенную компьютерную сеть и удостоверения подлинности электронной подписи.

В ключе использованы Java-технологии. Оперативная память устройства — 134 кбайт, ПЗУ — 64 кбайт. В компьютере-ключе могут храниться свыше 30 сертификатов с 1042-битными ключами наиболее часто используемого стандарта ISO X.509v3. Также в памяти суперключа может содержаться несколько сотен имен пользователя с соответствующими паролями, фотография, идентифицирующая владельца, данные о пользователе, которые обычно применяются для заполнения форм в Internet (например, при совершении покупок в онлайн-магазинах), электронная подпись владельца и биометрические данные (к примеру, отпечатки пальцев)

При попытке взлома на уровне данных доступ к информации о пользователе будет блокирован встроенным защитным программным обеспечением. Если ключик будут пытаться вскрыть физически, он получит сигнал о попытке вмешательства и сотрет всю информацию прежде, чем она попадет в руки взломщикам.

Все чаще для защиты от несанкционированного доступа стали применять программно-аппаратные комплексы, которыми могут быть оснащены рабочие станции компью-

терной сети и автономные компьютеры. В качестве примера рассмотрим комплексы защиты типа DALLAS LOCK.

Комплекс защиты DALLAS LOCK предназначен для исключения несанкционированного доступа к ресурсам компьютера и разграничения полномочий пользователей, а также для повышения надежности защиты входа в локальную сеть. Для идентификации пользователей служат электронные карты Touch Memory и личные пароли.

Программно-аппаратный комплекс DALLAS LOCK for Administrator предназначен для работы в вычислительных сетях совместно с комплексом DALLAS LOCK и представляет собой автоматизированное рабочее место администратора безопасности. Все модификации комплекса DALLAS LOCK возможно применять для защиты бездисковых рабочих станций локальной вычислительной сети. Эти комплексы можно использовать с различными операционными системами.

Запрос идентификатора при входе на персональный компьютер инициируется из ПЗУ на плате защиты до загрузки операционной системы, которая осуществляется только после предъявления зарегистрированного идентификатора (электронной карты) и вводе личного пароля. Поскольку идентификатор и пароль запрашиваются до обращения к дисководам, возможность загрузки с системной дискеты полностью исключена.

При инсталляции комплекса на жесткий диск обеспечивается гибкая настройка аппаратной части путем предварительного выбора адресного пространства ПЗУ платы защиты в свободной области адресов пользовательского BIOS, а также номера порта для работы с картой.

Поддерживается работа до 32 зарегистрированных пользователей на каждом компьютере, причем каждый из них может быть зарегистрирован на нескольких персональных компьютерах с разными полномочиями. Данные о пользователях хранятся в энергонезависимой памяти на плате защиты.

Энергонезависимая память платы защиты содержит образ системных областей компьютера, что позволяет контролировать их целостность.

Разграничение доступа пользователей возможно как по отношению к внешним устройствам (дисководам, LPT- и COM-портам), логическим дискам винчестера и таймеру, так и по времени работы на компьютере. Для каждого пользователя можно назначить свои права и уровни доступа к:

- системному диску C: (полный доступ; только для чтения);
- остальным логическим дискам винчестера (полный доступ; нет доступа; только для чтения);
- дисководам A: и B: (полный доступ; нет доступа; только для чтения);
- LPT- и COM-портам (полный доступ; нет доступа).

Время начала и окончания работы каждого пользователя на компьютере устанавливается администратором в пределах суток. Интервал времени, в течение которого пользователь может работать на компьютере со своими правами, может быть установлен от 1 минуты до 23 час. 59 мин (т. е. круглосуточно). Для предупреждения пользователя об истечении отведенного времени работы предусмотрен режим «будильника». За 5 мин до окончания сеанса работы пользователя выдается прерывистый звуковой сигнал. В пределах оставшихся 5 мин пользователь сможет закончить работу, после чего компьютер будет заблокирован. Предусмотрен режим защиты таймера от изменения системного времени.

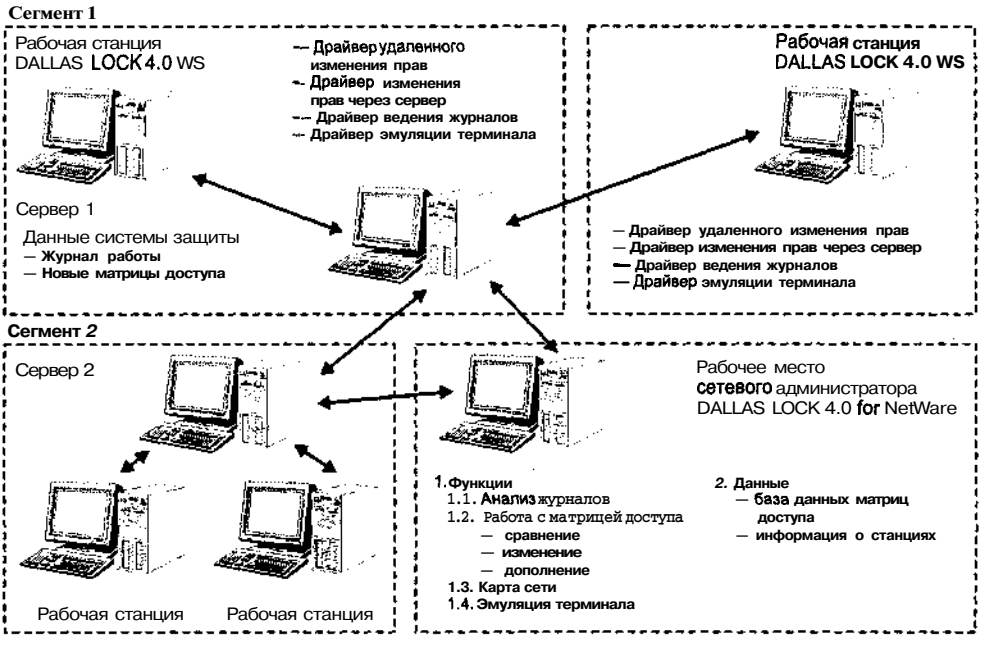


Рис. 3.19. Организация взаимодействия комплексов

При регистрации идентификатора комплекс создает для каждого пользователя индивидуальный файл AUTOEXEC, который запустится после загрузки компьютера пользователем с данной картой.

При выполнении процедуры входа на компьютер комплекс анализирует электронную карту и личный пароль пользователя. При этом в электронном журнале фиксируются номер предъявленной карты, имя пользователя, дата, время попытки «входа» и результат попытки (проход — отказ в доступе), а также причина отказа в загрузке компьютера в случае неудачи. В электронных журналах фиксируются действия пользователей по работе с файлами на дисках. Электронные журналы доступны только администратору. Пользователи могут самостоятельно менять личные пароли для входа на компьютер и для доступа к индивидуальным зашифрованным дискам винчестера.

Для усиления защиты информации на компьютере администратор может для всех или некоторых пользователей включать режим принудительной смены пароля входа. Пользователь будет вынужден сменить пароль входа после загрузки компьютера установленного числа раз.

Доступ к электронным журналам рабочих станций администратор безопасности получает на своем рабочем месте. Для передачи данных используются протоколы IPX, что позволяет размещать защищенные станции в различных сегментах (рис. 3.19).

Со своего рабочего места администратор получает список активных станций в сети, выбирает любую из них и запрашивает любой из журналов. После установления соединения журнал автоматически переписывается на диск компьютера администратора и обнуляется на рабочей станции. Данные из журналов могут быть выведены в файл

или на печать. В случае необходимости оперативного получения информации о событиях, происходящих на рабочей станции, администратор безопасности может негласно просматривать содержание ее экрана. Ему предоставляется возможность установить для любого пользователя режим полного стирания информации из памяти и с носителей при удалении файлов.

Комплекс DALLAS LOCK может быть установлен на любой IBM-совместимый компьютер, работающий автономно или в качестве рабочей станции локальной вычислительной сети. Для размещения файлов и работы комплекса требуется до 3 Мбайт пространства на системном разделе C: жесткого диска. ПЗУ платы защиты занимает 8 Кбайт в области памяти пользовательских BIOS.

Для создания на винчестере дополнительных зашифрованных индивидуальных дисков каждому пользователю на системном разделе C: необходимо предусмотреть пространство, равное суммарной емкости этих дисков. Максимальный объем каждого диска — 32 Мбайт.

Защита сети с помощью биометрических систем

Кто из нас не сталкивался с ситуацией, когда, подойдя к своему дому, обнаруживаешь, что ключи от двери забыл, случайно выронил или оставил где-то в толчее большого города.

Что же можно придумать, чтобы избежать таких ситуаций. Чего проще для открытия двери использовать то, что присуще самому человеку: голос, руки, глаза, отпечатки пальцев и т. д. Эти объекты, назовем их биометрическими идентификаторами, принадлежат человеку и являются его неотъемлемой частью. Их нельзя где-то забыть, оставить, потерять. Биометрия основывается на анатомической уникальности каждого человека, и, следовательно, это можно использовать для идентификации личности.

В последнее время быстро возрастает интерес к биометрическим системам идентификации пользователей компьютерных систем. Сферы применения технологий идентификации практически не ограничены. Правительственные и частные организации заинтересованы в технологиях распознавания лиц, поскольку это позволяет повысить уровень защиты секретной и конфиденциальной информации. Компании, работающие в области информационных технологий, заинтересованы в технологиях распознавания отпечатков пальцев, лиц, голоса, радужной оболочки глаза и т. п., чтобы предотвратить проникновение посторонних в их сети.

По словам президента Microsoft Билла Гейтса, «Биометрия в ближайшем будущем обязательно станет важнейшей частью информационных технологий... Технологии идентификации голоса, лица и отпечатков пальцев будут наиболее важными инновационными технологиями в ближайшие несколько лет».

Но уже и сейчас в компьютерных сетях есть сайты, доступ к которым регламентируется методами дактилоскопии, например, разработанные компанией Biometric Trancking. Совсем недавно разработана программа, которая снимает отпечатки пальцев клиента при помощи небольшого устройства. Будучи подключенной к браузеру Netscape Navigator, программа начинает функционировать только в том случае, если сайт, на который пытаются войти, требует дактилоскопии посетителя. Это средство предназначено для ужесточения мер безопасности, совместно с паролями, электрон-

ными карточками и т. п. Для непосредственного ввода данных об отпечатках пальцев используется специальный сканер TouchSafe II, изготовленный компанией Identix. Подключается этот сканер к персональному компьютеру через контроллер, подключенный к стандартной шине ISA.

Возможности установления личности человека по его биометрическим характеристикам известны давно и широко обсуждаются уже много лет. Тем не менее сегодня еще очень многие считают технику такой идентификации делом будущего и убеждены, что пока она остается уделом фантастических кинофильмов, поскольку практическое применение биометрических методов еще слишком дорого.

Способ опознавания личности с помощью особенностей строения человеческого тела придумали и применяли еще древнеегипетские фараоны. Чтобы идентифицировать личность человека, древние египтяне замеряли его рост. Распознавать отпечатки пальцев стали значительно позднее. Это одна из простейших и хорошо известных биометрических технологий. Коммерческие идентификационные системы автоматического распознавания отпечатков пальцев появились еще в 60-х годах XIX века. Но и до недавнего времени эти системы в основном использовались правоохранительными органами при расследовании преступлений. Первые системы биометрического контроля доступа производили идентификацию по длине пальцев.

Но кроме технологии распознавания отпечатков пальцев появились и другие биометрические технологии, в частности, распознавание черт лица (на основе оптического и инфракрасного изображений), руки, пальцев, радужной оболочки, сетчатки, подписи и голоса. Сейчас создаются и другие системы, позволяющие анализировать иные характеристики человека, такие как уши, запах тела, манера работы на клавиатуре и походка.

Биометрические характеристики человека уникальны. Большинство таких ключей нельзя скопировать и точно воспроизвести. Теоретически это идеальные ключи. Однако при использовании биометрической идентификации возникает множество специфических проблем. Поэтому рассмотрим биометрические системы идентификации более подробно.

Системы идентификации, анализирующие характерные черты личности человека, можно разделить (рис. 3.20) на две большие группы:

- физиологические;
- поведенческие (психологические).

Физиологические системы считаются более надежными, т. к. используемые ими индивидуальные особенности человека почти не изменяются под влиянием его психоэмоционального состояния. Физиологические системы идентификации личности имеют дело со статическими характеристиками человека — отпечатками пальцев, капиллярными узорами пальцев, радужной оболочкой и рисунком сетчатки глаза, геометрией кисти руки, формой ушной раковины, распознаванием черт лица (на основе оптического или инфракрасного изображений).

Поведенческие методы оценивают действия индивидуума, предоставляя пользователю некоторую степень контроля над его поступками. Биометрия, основанная на этих методах, учитывает высокую степень внутриличностных вариаций (например, настроение или состояние здоровья влияют на оцениваемую характеристику), поэтому такие методы лучше всего работают при регулярном использовании устройства. Поведен-

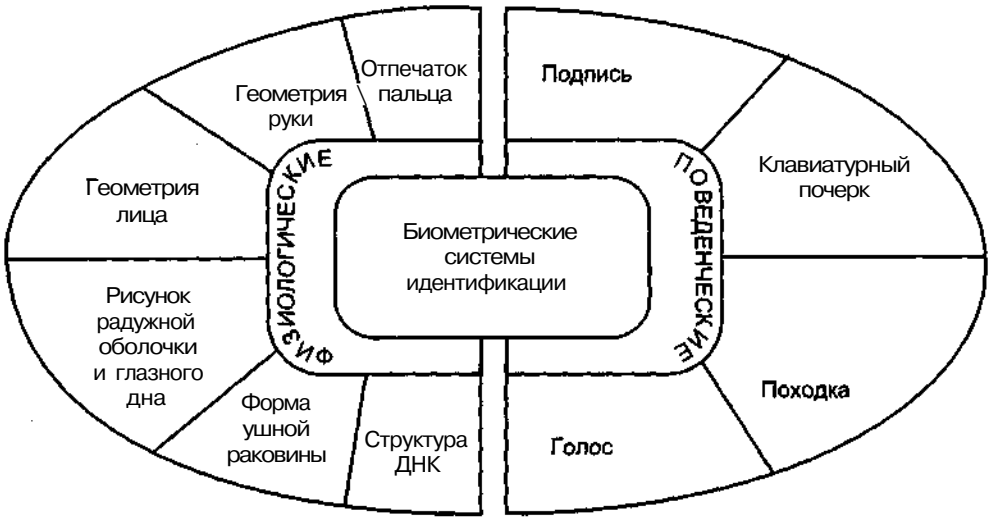


Рис. 3.20. Биометрические системы идентификации

ческие (или как их еще иногда называют — психологические) характеристики, такие как подпись, походка, голос или клавиатурный почерк, находятся под влиянием управляемых действий и менее управляемых психологических факторов. Поскольку поведенческие характеристики могут изменяться с течением времени, зарегистрированный биометрический образец должен обновляться при каждом его использовании. Хотя биометрия, основанная на поведенческих характеристиках, менее дорога и представляет меньшую угрозу для пользователей, физиологические черты позволяют идентифицировать личность с высокой точностью. В любом случае оба метода обеспечивают значительно более высокий уровень идентификации, чем пароли или карты.

Поскольку биометрические характеристики каждой отдельной личности уникальны, то они могут использоваться для предотвращения НСД с помощью автоматизированного метода биометрического контроля, который путем проверки (исследования) уникальных физиологических особенностей или поведенческих характеристик человека идентифицирует личность.

Кроме этого, биометрические системы идентификации личности различаются (рис. 3.21) еще по ряду показателей:

- пропускная способность;
- стоимость;
- надежность с позиции идентификации;
- простота и удобство в использовании;
- степень психологического комфорта;
- возможность обмана системы;
- способ считывания;
- точность установления аутентичности;
- увеличенная производительность;
- затраты на обслуживание;

Рис. 3.21. Показатели биометрических систем

- интеграция;
- конфиденциальность.

Пропускная способность системы в этом случае характеризуется временем, необходимым для обслуживания одного пользователя. Она зависит, в частности, от режима работы устройства (производится идентификация или аутентификация). При идентификации пользователя требуется больше времени, чем для аутентификации, т. к. необходимо сравнить с образцом почти все эталоны из базы данных. В режиме аутентификации пользователь должен набрать на клавиатуре свой персональный код (номер эталона в базе данных), и системе достаточно сравнить предъявляемый образец с одним эталоном. Во многих системах эти режимы может выбрать администратор.

Стоимость является одним из определяющих факторов широкого использования биометрических систем. Стоимость этих систем достаточно высока в самих странах-производителях и значительно возрастает, когда системы доходят до конечных потребителей в России. Тут сказываются и таможенные тарифы, и прибыль, закладываемая продавцами.

Несколько лучше в ценовом аспекте обстоят дела с отечественными разработками. Причем качество идентификации многих из них выше западных аналогов. Это и не удивительно, ведь наши разработчики всегда славились недюжинной смекалкой и мастерством. Одна же из серьезных проблем, сдерживающих распространение наших разработок, — уровень производства, не позволяющий выйти на зарубежный рынок.

Говоря о надежности биометрической системы с позиции идентификации, мы имеем две вероятности. Речь идет о вероятности «ложных отказов» (система не признала своего) и «ложных допусков» (система приняла «чужого» за «своего»). Это особенно трудная и сложная область биометрии, т. к. система должна пропускать меньшее число самозванцев и в то же время отвергать меньшее число законных пользователей.

Простота и удобство в использовании во многом определяют потребительские свойства биометрических систем. Ведь все часто задают следующие вопросы. Насколько легко установить данную биометрическую систему? Требует ли система активного участия пользователя или получение характеристик слишком обременительно? Требует ли система длительного обучения? Не произойдет ли так, что обременительная или громоздкая биометрическая система аутентификации будет отвергнута так же, как мы отказываемся от использования систем, требующих ввода длинных паролей?

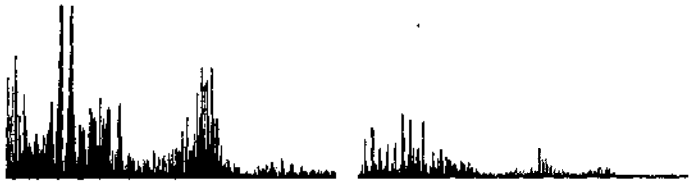
Степень психологического комфорта определяет, насколько те или иные системы и методы определения биометрических характеристик способны вызвать у пользователей негативную реакцию, страх или сомнение. Например, отдельные люди опасаются, скажем, дактилоскопии, а другие не желают смотреть в глазок видеокамеры с лазерной подсветкой.

Возможность обмана системы связана с использованием различных «дубликатов»: слепков, магнитофонных записей и т. д. Наиболее «легковерными» считаются системы опознания по лицу и голосу.

Способ считывания определяет, нужно ли пользователю прикладывать свой палец к считывателю, прислоняться лицом к окуляру и т. п. или достаточно продемонстрировать «электронному» привратнику атрибут, необходимый для идентификации, например, произнести условную фразу или посмотреть в объектив видеокамеры. Исходя из этого, различают два способа считывания — дистанционный и контактный. Технология дистанционного считывания позволяет увеличить пропускную способность, избежать регулярной очистки считывателя и исключить его износ, увеличить вандалозащищенность и т. п.

Точность аутентификации при использовании биометрических систем несколько отличается от точности систем, использующих пароли. Предоставление корректного пароля в системе аутентификации по паролю всегда дает корректный результат о подтверждении подлинности. Но если в биометрическую систему аутентификации представлены законные (настоящие) биометрические характеристики, это, тем не менее, не гарантирует корректной аутентификации. Такое может произойти из-за «шума» датчика, ограничений методов обработки и, что еще важнее, изменчивости биометрических характеристик (рис. 3.22). Есть также вероятность, что может быть подтверждена подлинность человека, выдающего себя за законного пользователя. Более того, точность данной биометрической реализации имеет немаловажное значение для пользователей, на которых рассчитана система. Для успешного применения биометрической технологии с целью идентификации личности важно понимать и реально оценивать эту технологию в контексте приложения, для которого она предназначена, а также учитывать состав пользователей этого приложения.

Производительность зависит от таких параметров, как точность, стоимость, интеграция и удобство использования.



Голосовые характеристики

Отпечатки пальцев

Подпись

Рис. 3.22. Изменчивость биометрических характеристик

Для многих приложений, таких как регистрация в персональном компьютере или сети, важное значение имеют дополнительные расходы на реализацию биометрической технологии. Некоторые применения (например, регистрация в мобильных компьютерах) не позволяют использовать громоздкое аппаратное обеспечение биометрических датчиков, тем самым стимулируя миниатюризацию таких устройств. Учитывая появление множества недорогих, но мощных систем, крупномасштабного производства дешевых датчиков, становится возможным использовать биометрику в новых приложениях идентификации личности, а за счет этого, в свою очередь, снижаются цены на них.

Для улучшения характеристик опознавания систем идентификации все шире применяется интеграция нескольких биометрических систем в одном устройстве. Аутентификация совершенно бессмысленна, если система не может гарантировать, что законный пользователь действительно представил необходимые характеристики. Применение нескольких биометрик позволяет снять остроту других проблем в области идентификации личности по ее биометрическим характеристикам.

К примеру, часть пользователей, на которых ориентирована конкретная система, или не могут представить конкретный биометрический идентификатор, или предоставляемые данные могут оказаться бесполезными. Более того, определенные биометрики могут оказаться неприемлемыми для части пользователей.

Несмотря на очевидные преимущества, существует несколько негативных предубеждений против биометрии, которые часто вызывают вопросы о конфиденциальности информации в этих системах. Иными словами, не будут ли биометрические данные ис-

пользоваться для слежки за людьми и нарушения их права на частную жизнь. Чтобы обеспечить социально-правовую защиту пользователя, многие зарубежные производители считывателей условились хранить в базе данных не изображение отпечатка, а некоторый полученный из него ключ, по которому восстановление отпечатка невозможно.

Рассмотрим, как же работает любая биометрическая система, использующая физиологические или поведенческие характеристики человека.

Основа любой биометрической системы опознавания личности — датчик, который выдает сигнал, промодулированный в зависимости от физических особенностей конкретного человека. Далее происходит преобразование аналогового сигнала в цифровой формат, удаляется вся ненужная информация и полученная матрица (шаблон) сохраняется в памяти. Современные системы опознавания по отпечаткам пальцев, например, имеют матрицу объемом менее 100 байт. Вместо информации об отпечатках пальцев может использоваться информация о всей ладони или о венозном рисунке запястья, о радужной оболочке глаз. Данная информация может совмещаться с информацией о голосе, почерке, походке. Биометрическая система — это система распознавания шаблона, которая устанавливает аутентичность конкретных физиологических или поведенческих характеристик пользователя. Логически биометрическая система (рис. 3.23) может быть разделена на два модуля:

- модуль регистрации;
- модуль идентификации.

Модуль регистрации отвечает за «обучение» системы идентифицировать конкретного человека. На этапе регистрации биометрические датчики сканируют изображение лица человека для того, чтобы создать его цифровое представление. Специальный модуль обрабатывает это представление, чтобы выделить характерные особенности и сгенерировать более компактное и выразительное представление, называемое шаблоном. Для изображения лица такими характерными особенностями могут стать размер и расположение глаз, носа и рта. Шаблон для каждого пользователя хранится в базе данных биометрической системы. Эта база данных может быть централизованной или распределенной, когда шаблон каждого пользователя сохраняется на смарт-карте и передается пользователю.

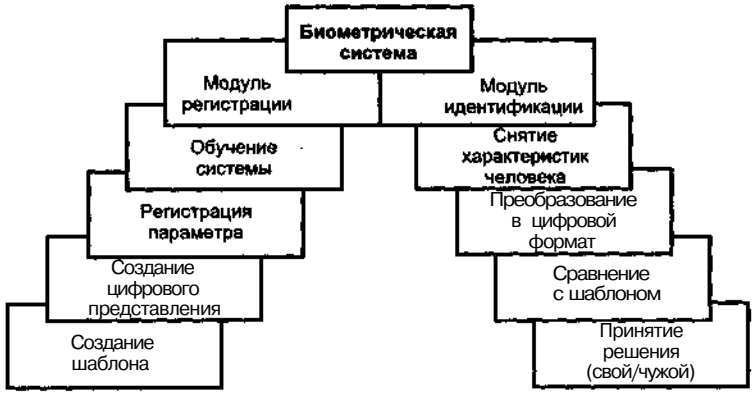


Рис. 3.23. Состав биометрической системы

Модуль идентификации отвечает за распознавание пользователя компьютера. На этапе идентификации биометрический датчик снимает характеристики человека, идентификация которого проводится, и преобразует эти характеристики в тот же цифровой формат, в котором хранится шаблон. Полученный шаблон сравнивается с хранимым шаблоном, чтобы определить, соответствуют ли эти шаблоны друг другу.

Идентификация может выполняться в виде верификации, аутентификации (проверка утверждения типа «Я — Сергей Иванов») или распознавания, определяя личность человека из базы данных о людях, известных системе (определение того, кто я, не зная моего имени). В верификационной системе, когда полученные характеристики и хранимый шаблон пользователя, за которого себя выдает человек, совпадают, система подтверждает идентичность. Когда полученные характеристики и один из хранимых шаблонов оказываются одинаковыми, система распознавания идентифицирует человека с соответствующим шаблоном.

Рассмотрим более подробно опознавательные методы (физиологические), как наиболее часто используемые в системах идентификации личности.

Идентификация по отпечатку пальца

Один из простейших и хорошо известных биометрических методов идентификации личности — распознавание отпечатков пальцев. Именно он оказался наиболее практичным в отношении реализации и восприятия его людьми и именно он используется уже длительное время.

Отпечатки пальцев у всех людей совершенно разные. Все люди, населяющие в наше время Землю, имеют, присущие только им одним, определенные отпечатки пальцев. И даже отпечатки пальцев всех предшествующих поколений людей также отличны от всех последующих. Правоохранительные органы во всем мире используют идентификацию по отпечаткам пальцев уже более ста лет, причем до нынешнего дня не выявлено ни одного случая совпадения отпечатков пальцев у разных людей, включая даже однояйцевых близнецов.

В силу этого именно отпечатки пальцев руки одного человека считаются специфической, присущей только этому человеку «личной карточкой», и именно в таком качестве это свойство применяется во всем мире.

Но такая особенность пальцев руки человека была обнаружена лишь к концу девятнадцатого столетия. До того времени они представлялись людям просто набором линий, ничего не обозначавшими и не обладавшими какими-либо особенностями. Кожа человека состоит из двух слоев, при этом нижний слой образует множество выступов — сосочков (от лат. papillae — сосочек), в вершине которых имеются отверстия выходных протоков потовых желез. На основной части кожи сосочки (потовые железы) располагаются хаотично и трудно наблюдаемы. На отдельных участках кожи конечностей папилляры строго упорядочены в линии (гребни), образующие уникальные папиллярные узоры. Эти узоры и отражают всю человеческую индивидуальность. Существует всего три основный типа (рис. 3.24) узора отпечатка пальца различной степени сложности:

- высокой (завитки);
- средней (петлевые или круговые);
- низкой (дуговые).

Идея идентификации личности на основе папиллярных рисунков пальцев рук предложена двумя авторами — Г. Фулдсом и В. Гершелем — в статье авторитетного английского журнала «Nature» в 1880 году. В 1864 году доктор Нейман Гроу опубликовал первые работы с предложением идентификации личности по отпечаткам пальцев. ФБР в конце прошлого века предприняло первые шаги в этом направлении.

В 1895 году дактилоскопия как метод регистрации преступников введена в Англии. А уже в 1905 году в Лондонском суде был юридический прецедент, когда подсудимый был приговорен к смертной казни на основании идентификации отпечатков его пальцев.

В России дактилоскопия как метод регистрации преступников стала использоваться с 1907 года.

Данный метод идентификации широко распространен в криминалистике, что является причиной настороженного отношения к нему части населения. А вот в США, например, дактилоскопия проводится у всего населения и не вызывает предубеждения, характерного для жителей других стран.

Современные сенсоры отпечатков пальцев точнее и эффективнее в обработке необходимой информации, чем их более ранние аналоги. Кроме того, цены на них значительно ниже, чем на другие биометрические устройства.

В устройствах для сканирования отпечатков пальцев используется несколько подходов, в том числе оптические, микросхемные и ультразвуковые технологии. Преимуществом ультразвукового сканирования является возможность определить требуемые характеристики на грязных пальцах и даже через тонкие резиновые перчатки. Кроме того, все устройства считывания различаются по виду, как, например, внешние сканеры для рабочих станций, ноутбуков и портативных компьютеров. Встроенные сканеры отпечатков пальцев для этих типов систем также начинают появляться, как и сканеры отпечатков для сотовых телефонов.

Преимущества доступа по отпечатку пальца — это простота использования, удобство и надежность. Весь процесс идентификации занимает мало времени и не требует усилий от тех, кто использует данную систему доступа.

В любой такой системе клиенту сначала предлагают приложить свой палец (любой) к окошку распознающего устройства. На первом этапе информация, полученная от изображения пальца, используется для формирования так называемого шаблона.

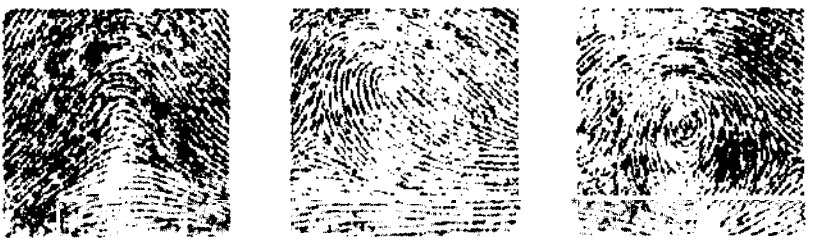


Рис. 3.24. Типы рисунков отпечатка пальца

Эта операция занимает 10—15 с. Потом система предлагает человеку предъявить палец еще несколько раз, чтобы проверить пригодность занесенной в память информации. Процесс регистрации занимает несколько минут. Основным элементом устройства является сканер, считывающий папиллярный узор, который затем обрабатывается с помощью специального алгоритма, и полученный код сравнивается с шаблоном, хранящимся в памяти.

Существует два основных алгоритма сравнения: по характерным точкам и рельефу всей поверхности пальца. Первый алгоритм выявляет характерные участки и запоминает их взаиморасположение. Во втором случае анализируется вся «картина» в целом. При распознавании по характерным точкам возникает шум высокого уровня, если палец в плохом состоянии. При распознавании по всей поверхности этого недостатка нет, но есть другой: требуется очень аккуратно размещать палец на сканирующем элементе. В современных системах используется также комбинация обоих алгоритмов, за счет чего повышается уровень надежности системы.

Сформированный шаблон заносится в базу данных системы, в память главного компьютера или микропроцессорной карточки, либо в иное устройство хранения цифровых данных и получается некий цифровой индекс. Объем хранимой эталонной информации может быть существенно уменьшен, если сделать классификацию по характерным типам папиллярных рисунков и выделить на отпечатке микроособенности, представляющие собой начала (окончания) папиллярных линий или их слияния (разветвления). В предлагаемых на рынке средствах идентификации по отпечатку пальца информация об отпечатках, хранимая в базе данных оператора системы, как правило, недостаточна для полной реконструкции отпечатка. Это **важно**, поскольку исключается использование такой информации в каких-либо иных целях, например, при расследовании преступления.

В некоторых системах можно зарегистрировать отпечатки нескольких пальцев одного человека, повторив процесс регистрации для каждого пальца, который вы захотите использовать для идентификации, но каждый палец можно зарегистрировать только один раз.

Метод распознавания отпечатков пальцев относится к числу одних из самых надежных и безопасных биометрических способов идентификации. Но далеко не всегда необходима высшая степень безопасности (разве что при использовании правоохранительными органами или на сверхсекретных объектах), а порой и не всегда желательна, поэтому в коммерческих системах предусмотрена возможность регулировать порог идентификации и, следовательно, изменять степень безопасности системы. Для практического применения система идентификации по отпечатку пальца должна обладать следующими показателями:

- доля случаев ошибочной идентификации — не более **0,0001%;**
- G доля ошибочных отказов в идентификации с первой попытки — не более 1%;
- время идентификации — не более 5 с.

Кроме того, все коммерческие системы должны быть обязательно испытаны независимыми организациями.

Вероятность ошибочного отказа в идентификации зависит в основном от поведения клиента и одновременно является наиболее важным, с точки зрения клиента, рабочим параметром идентифицирующей системы. Возможность ошибочного отказа в

идентификации часто считают одним из существенных недостатков биометрических систем. Очень легко получить отказ в доступе, предъявив не тот палец или неправильно приложив его к окошку распознающего устройства. В связи с этим обычно допускаются три попытки, и после первого отказа клиент, как правило, понимает, что допустил ошибку, и относится к процедуре идентификации более аккуратно. Таким образом, вероятность ошибочной неидентификации клиента становится практически равной вероятности ложной идентификации и составляет около 0,0001%.

Еще один аспект безопасности рассматриваемых систем связан с использованием различных фальшивок. Заказчики часто требуют от поставщиков, чтобы система распознавала случаи предъявления слепков пальцев, выполненных, например, из силикона. Ни одна из систем идентификации по отпечатку пальца не обеспечивает надежной защиты от подделок. Можно лишь рассчитывать на то, что сделать хороший слепок совсем не так просто, и в большинстве случаев для этого необходимо соучастие зарегистрированного человека. Тем не менее, для защиты от предъявления фальшивого пальца предпринимаются различные меры.

Первая мера — анализ цветового спектра предъявляемого пальца, что позволяет отказывать в идентификации предъявителям простейших слепков.

Вторая мера основана на оценке коэффициента отражения вещества, прижатого к окошку распознающего устройства, что позволяет отвергать материалы, из которых обычно делаются слепки. Хотя ни тот, ни другой из дополнительных тестов не дают 100% надежности, они все же обеспечивают высокую вероятность выявления фальшивок.

Порезы и другие повреждения пальца, использованного для регистрации, могут в некоторых случаях исключить возможность идентификации. Именно во избежание таких случаев система должна зарегистрировать несколько пальцев.

Встречаются люди, пальцы которых практически не имеют рельефа. В большинстве таких случаев можно найти палец, который система регистрирует нормально. Другой выход состоит в снижении порога идентификации для данного конкретного человека. При этом общий уровень безопасности системы снижаться не должен.

Есть еще ряд требований к состоянию руки. Например, влажность. Отдельные устройства при сухом или мокром пальце часто выдают «ложные отказы». Еще один недостаток дактилоскопической системы идентификации — рука должна быть чистой. Отдельные модели считывателей капризны и в отношении температуры кисти.

Современные сканеры отпечатков пальцев имеют небольшие размеры, недороги и могут быть легко приспособлены к разным задачам. Компьютерный вариант считывателя может быть встроен в клавиатуру, периферийное устройство, например, мышь (рис. 3.25) или выполнен в виде отдельного выносного устройства.

Устройство обработки изображения, предназначенное для идентификации отпечатков пальцев FIU (Fingerprint Identification Unit) корпорации Sony, например, включает в себя собственный микропроцессор и память, выполняющие полную обработку изображений. Это устройство подключается к персональному компьютеру через последовательный порт и может хранить в памяти до 1000 отпечатков пальцев.

Компания Digital Persona выпускает систему доступа по отпечаткам пальцев U.are.U. Пакет U.are.U Pro Workstation Package включает сенсор отпечатков пальцев, программное обеспечение рабочей станции, комплект приложений для регистрации, разблокирования и доступа в Internet одним касанием, а также консоль администратора.

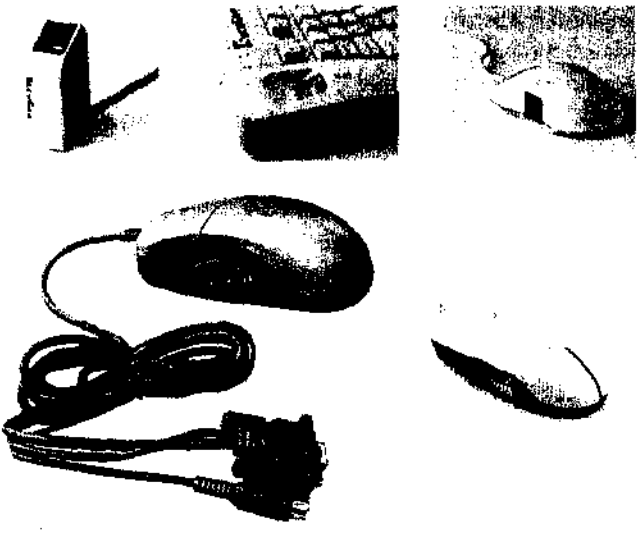


Рис. 3.25. Варианты считывателей отпечатков пальцев

U.are.U Pro Server Software поддерживает централизованную регистрацию, идентификацию на сервере и роуминг пользователей. С помощью программного обеспечения Private Space пользователь может шифровать и дешифровать данные на лету, просто прикоснувшись к сенсору.

Fingerprint Identification Reader компании Compaq Computer включает программное обеспечение Biologon от компании Identicator. Система предусматривает также факультативную поддержку Deskpro PC компании Compaq. Модуль с небольшой камерой размещается на персональном компьютере. Камера снимает изображение отпечатка пальца пользователя, после чего оно конвертируется, шифруется и сохраняется в сети.

Идентификационная периферия 5th Sense компании Veridicom создана на базе ее собственного FPSno Silicon Fingerprint Sensor. Эти подключаемые устройства могут использоваться на настольных и портативных системах. Программное обеспечение Imaging Suite захватывает и конвертирует изображение, а Verification Suite анализирует качество изображения, преобразует его в двоичную форму и извлекает необходимые данные.

FingerLoc AF-Si Sensor от AuthenTec поставляется *с* программным обеспечением с поддержкой таких функций, как автоматическая калибрация и оптимизация изображения. Сенсорная микросхема непосредственно взаимодействует с главным процессором компьютера во время идентификации. На этом же компьютере выполняются программы извлечения и сопоставления данных.

Компания SAC Techologies представила новейшую систему SACcat шестого поколения, предназначенную для идентификации личности с использованием биометрических показателей. В этой системе применяется новый запатентованный компанией алгоритм Vector Segment, который преобразует отпечаток пальца в математическое представление BioKEY, дающее возможность сформировать персонализированную цифровую подпись, уникальную для каждого человека.

Возможностям применения цифровой подписи BioKEY нет числа: ее можно использовать для контроля доступа к информационным системам или на территорию предприятий, в Internet, в электронной торговле и в других случаях, когда требуется идентификация личности. При этом не нужны идентификационные номера, пароли, PIN-коды, ключи и карточки.

Компания Intel представила весьма интересный подход к проблеме защиты портативных компьютеров, о которой хотя и не принято говорить, но известно во всех организациях. Аутентификация до загрузки операционной системы — самый логичный способ защитить данные на мобильном компьютере.

Предлагается следующий сценарий работы. Мобильные компьютеры, снабженные соответствующей функцией, требуют от пользователей подтвердить свою личность, как только проинициализированы процессор, набор микросхем, память и другие компоненты платформы.

Пользователи могут подтвердить свою личность с помощью сканеров отпечатков пальцев, смарт-карт и даже обычных паролей. Информация, получаемая таким образом, сравнивается с данными, которые хранятся в отдельной защищенной области памяти на компьютере.

Как только личность пользователя подтверждена, программный «ключ», размещенный в защищенной области, «открывает» жесткий диск и операционную систему.

Ноутбуки, наделенные такими возможностями, будут требовать подтверждения личности с помощью таких биометрических устройств, как сканеры отпечатков пальцев, прежде чем будет загружена операционная система. Сейчас большинство процедур аутентификации выполняется только после завершения загрузки и инициации работы операционной системы.

Из-за необходимости подтверждать свою личность до загрузки операционной системы пользователи, не имеющие соответствующих полномочий, не смогут работать с компьютером. Спецификация, предложенная корпорацией, определяет интерфейс, который производители BIOS (микропрограмм, помогающих аппаратным компонентам машины взаимодействовать с операционной системой) и устройств биометрической защиты могут использовать для организации подобного способа обеспечения безопасности. Первые мобильные компьютеры, обладающие такими функциями, уже выпущены.

Идентификация по кисти руки

При идентификации по кисти руки используются такие ее параметры, как геометрия, объемное изображение, рисунок кровеносных сосудов и т. п.

Метод распознавания геометрии кисти руки основан на анализе трехмерного изображения кисти руки и получил развитие в связи с тем, что математическая модель идентификации по данному параметру требует достаточно малого объема информации — всего 9 байт, что позволяет хранить большой объем записей, и следовательно, быстро осуществлять поиск. Однако форма кисти руки также является параметром, который достаточно сильно подвержен изменениям во времени, а кроме того, требует сканеров большого размера, что ведет к удорожанию системы.

В настоящее время, метод идентификации пользователей по геометрии руки используется многими организациями и компаниями. В некоторых случаях работать с отпечатком руки гораздо удобнее, чем с отпечатком пальца. Преимущества идентифи-

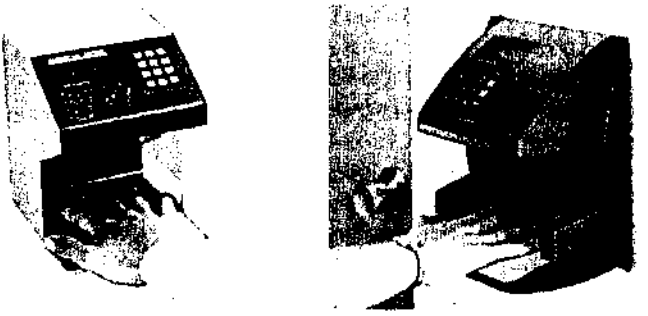


Рис. 3.26. Сканирующее устройство HandKey компании Recognition Systems

кации по геометрии ладони сравнимы с достоинствами идентификации по отпечатку пальца в вопросе надежности, хотя устройство для считывания отпечатков ладоней занимает больше места.

Наиболее удачное устройство, HandKey (рис. 3.26) производства компании Recognition Systems, измеряет геометрию руки. Для этого оно сканирует как внутреннюю, так и боковую сторону руки, используя встроенную видеокамеру и алгоритмы сжатия. Эти сканеры целесообразно применять в таких случаях ограничения доступа, когда из-за грязи или травм сканирование пальцев может быть проблематичным. Сканеры этой группы были установлены, например, в Олимпийской деревне в Атланте в 1996 году. И зарекомендовали себя очень хорошо.

Устройства, которые могут сканировать и другие параметры руки, находятся в процессе разработки несколькими компаниями, такими как BioMet Partners, Palmetrics и BTG.

Первое коммерческое биометрическое устройство, определяющее геометрию пальцев, появилось более 30 лет назад. Оно измеряло длину пальцев и применялось для табельного учета в компании Shearson Plc.

Первые модели считывателей, в которых в качестве идентификатора использовалось объемное изображение ладони, появились в 1972 году в США. Ладонь подсвечивалась множеством лампочек, расположенных в виде матрицы, и анализировалась тень — двухмерное изображение кисти руки. В современных моделях считывателей учитывается и толщина ладони.

Более сложными являются системы, дополнительно измеряющие профиль руки (объем пальцев, объем кисти, неровности ладони, расположение складок кожи на сгибах). Данные о трехмерной геометрии руки получают путем использования одной телевизионной камеры и инфракрасной подсветки руки под разными углами. Последовательное включение нескольких подсвечивающих светодиодов дают теневые варианты проекций трехмерной геометрии кисти руки, содержащие информацию о ее объеме. Устройства, в которых реализовано подобное техническое решение, не будут малогабаритными, так как требуется выносить источники подсветки на расстояние 10—15см.

Широкому распространению таких систем препятствует несколько факторов: высокая цена самого считывателя; невысокая пропускная способность — ладонь нужно правильно расположить в считывающем устройстве; отсутствие технологий защиты от фальсификации; вместо кисти руки в считыватель можно засунуть ее муляж. Прав-

да, у этой системы биометрической идентификации есть и свои преимущества. В отличие от дактилоскопических считывателей, они не предъявляют повышенных требований к влажности, температуре, цвету, загрязненности и другим параметрам. Системы такого типа целесообразно применять в студенческих городках, на складах и т. п., то есть там, где невозможно обеспечить чистоту рук и относительно невысоки требования к безопасности.

Еще один вариант применения в качестве идентификатора кисть руки — это использование рисунка кровеносных сосудов на обратной стороне ладони. Такой узор уникален, его можно считывать на расстоянии и сложно воспроизвести искусственно. Эта передовая технология распознавания лежит в основе устройства BK-300S. Особенность прибора заключается в том, что оно сканирует не поверхность пальца, а устройство внутренних органов человека (структуру сети кровеносных сосудов руки) с помощью специального инфракрасного датчика. В этом случае деформация поверхности, сухость, влажность или загрязненность рук никак не влияют на результаты распознавания. После сканирования система распознавания обрабатывает полученное изображение. Устройство BK-300S может работать как самостоятельно, так и в сети под управлением BK-сервера. **BK-сервер** поддерживает не только устройства серии BK, но и множество других охранных устройств.

Кроме рассмотренных устройств, существуют такие, которые используют для идентификации личности рисунок вен, расположенных на тыльной стороне кисти руки, сжатой в кулак. Наблюдение рисунка вен осуществляется телевизионной камерой при инфракрасной подсветке, после чего вычисляется шаблон.

Идентификация по лицу

Система распознавания по лицу — наиболее древний и распространенный способ идентификации. Именно такой процедуре подвергается каждый, кто пересекает границу. При этом пограничник сверяет фото на паспорте с лицом владельца паспорта и принимает решение, его это паспорт или нет. Примерно такую же процедуру выполняет компьютер, но с той лишь разницей, что фото уже находится в его памяти. Привлекательность данного метода основана на том, что он наиболее близок к тому, как мы идентифицируем друг друга. Развитие данного направления обусловлено быстрым ростом мультимедийных видеотехнологий, благодаря которым можно увидеть все больше видеокамер, установленных дома и на рабочих местах.

Существенный импульс это направление получило с повсеместным распространением технологии видеоконференций **Internet/intranet.** Ориентация на стандартные видеокамеры персональных компьютеров делает этот класс биометрических систем сравнительно дешевым. Тем не менее, идентификация человека по геометрии лица представляет собой достаточно сложную (с математической точки зрения) задачу. Хотя лицо человека — уникальный параметр, но достаточно динамичный; человек может улыбаться, отпускать бороду и усы, надевать очки — все это добавляет трудности в процедуре идентификации и требует достаточно мощной и дорогой аппаратуры, что соответственно влияет на степень распространенности данного метода.

Алгоритм функционирования системы опознавания достаточно прост. Изображение лица считывается обычной видеокамерой и анализируется. Программное обеспечение сравнивает введенный портрет с хранящимся в памяти эталоном. Некоторые системы дополнительно архивируют вводимые изображения для возможного в будущем разбора конфликтных ситуаций. Весьма важно также то, что биометрические системы этого класса потенциально способны выполнять непрерывную идентификацию (аутентификацию) пользователя компьютера в течение всего сеанса его работы. Большинство алгоритмов позволяет компенсировать наличие очков, шляпы и бороды у исследуемого индивида. Было бы наивно предполагать, что с помощью подобных систем можно получить очень точный результат. Несмотря на это, в некоторых странах они довольно успешно используются для верификации кассиров и пользователей депозитных сейфов.

Основными проблемами, с которыми сталкиваются разработчики данного класса биометрических систем, являются изменение освещенности, вариации положения головы пользователя, выделение информативной части портрета (гашение фона). С этими проблемами удается справиться, автоматически выделяя на лице особые точки и затем измеряя расстояния между ними. На лице выделяют контуры глаз, бровей, носа, подбородка. Расстояния между характерными точками этих контуров образуют весьма компактный эталон конкретного лица, легко поддающийся масштабированию. Задача оконтуривания характерных деталей лица легко может быть решена для плоских двухмерных изображений с фронтальной подсветкой, но такие биометрические системы можно обмануть плоскими изображениями лица-оригинала. Для двухмерных систем изготовление муляжа-фотографии — это не сложная техническая задача.

Существенные технические трудности при изготовлении муляжа возникают при использовании трехмерных биометрических систем, способных по перепадам яркости отраженного света восстанавливать трехмерное изображение лица. Такие системы способны компенсировать неопределенность расположения источника освещенности по отношению к идентифицируемому лицу, а также неопределенность положения лица по отношению к видеокамере. Обмануть системы этого класса можно только объемной маской, точно воспроизводящей оригинал.

Данный метод обладает существенным преимуществом: для хранения данных об одном образце идентификационного кода (одном лице) требуется совсем немного памяти. А все потому, что, как выяснилось, человеческое лицо можно поделить на относительно небольшое количество «блоков», неизменных у всех людей. Этих блоков больше, чем известных нам частей лица, но современная техника научилась выделять их и строить на их основе модели, руководствуясь взаимным расположением блоков.

Например, аппаратура компании Visionics использует метод обработки локальных участков изображения лица, и для вычисления уникального кода каждого человека ей требуется всего от 12 до 40 характерных участков. Полученный код выражается в виде сложной математической формулы.

FaceIt — одна из лучших в мире программ, которая позволяет распознавать лицо. Она находит промышленное применение в целом ряде приложений. Технология успешно реализована не только на рабочих станциях, но и на мобильных компьютерах, поскольку появилась технология FaceIt для Pocket PC.

Технология FaceIt компании Visionics, входящая в Authentication Suite компании BioNetrix, представляет собой программный механизм распознавания черт лица со сжатием изображения до 84 байт. Среди поддерживаемых функций — генерация отпечатка лица в виде уникального цифрового кода; сегментация для отделения изображения лица от фона; отслеживание изменений в лице с течением времени.

Технология идентификации геометрии лица может использоваться, в частности, для такой экзотической цели, как слежение. Алгоритм позволяет выделять изображение лица на некотором расстоянии и на любом фоне, даже состоящем из других лиц, чтобы затем сравнить его с хранящимся в памяти эталонным кодом. Система была испытана для выявления преступников на чемпионате США по американскому футболу. Факт применения этой системы скрывали до конца чемпионата, и зрители пришли в негодование от такого посягательства на демократические свободы. Технология состояла в преобразовании фотографии лица в математическое выражение, описывающее геометрию его черт. Система переводила изображение в 84-разрядный файл, называемый face print. Затем файлы, полученные при помощи видеокамер во время матчей, сравнивались с face print известных преступников. Хотя несанкционированное применение такой технологии, равно как и сама технология, подверглись осуждению со стороны общественности, правоохранительные органы ряда городов уже выделили средства для ее развертывания.

Программный продукт FaceMe является аналогом FaceIt и решает задачи верификации и идентификации человека на основе анализа структуры его лица. Для успешной работы SPIRIT FaceMe необходимо затратить менее минуты для регистрации вашего лица.

Система One-on-One Facial Recognition основана на распознавании уникальных черт человеческого лица и позволяет контролировать доступ в здание или помещение.

Программа One-on-One, используя камеру, распознает лица и обеспечивает «ненавязчивый» контроль над пользователем. При инсталляции системы пользователь должен зарегистрировать свое лицо в базе данных. В результате этой процедуры One-on-One создаст цифровой шаблон (подпись), связанный с изображением лица. При дальнейшем использовании системы она будет проверять, совпадает ли изображение лица (вернее — шаблон) пользователя с хранящимся в базе.

Наличие косметики не влияет на работу системы распознавания, которая распознает людей даже в тех случаях, когда они решили отказаться от очков.

One-on-One не сохраняет изображение лица. Поэтому компьютерный взломщик не может реконструировать изображение по учетной записи в базе данных.

Цифровой шаблон или персональный идентификационный вектор (ПИВ), связанный с изображением лица, состоит из 96 байт. Его можно с легкостью сохранить на смарт-карте или в базе данных. Процесс распознавания лица занимает меньше одной секунды.

Фирма Neurodynamics сообщила о выходе биометрического пакета Tridentity, который использует распознавание лица для приложений электронной коммерции. Данная система строит и сохраняет в памяти трехмерную карту топографии лица пользователя. Впоследствии на основе этих данных Tridentity, как заявляют разработчики, позволяет успешно распознавать лица, видимые под любым углом. Способность алгоритма выделять индивидуальные особенности, такие как структура лицевых костей

Рис. 3.27. Термограмма лица человека

вокруг глаз и носа, обеспечивают его применимость, даже если для анализа доступны всего 10% поверхности лица, а также если черты искажены мимикой. Предполагается, что данное программное обеспечение можно будет использовать и в полицейских структурах для опознавания разыскиваемых преступников.

NVisage — это наиболее продвинутая разработка Cambridge Neurodynamics. Уникальность продукта заключается в том, что он ориентирован на распознавание трехмерных объектов, в то время как в большинстве современных устройств используется только двухмерная техника.

Двухмерные системы распознавания надежны только в том случае, когда известен угол поворота головы и расстояния до глаз, рта, носа и т. д. Когда человек находится в движении, двухмерная система становится в значительной степени зависимой от позы объекта распознавания. Благодаря Nvisage можно значительно повысить надежность распознавания.

При использовании источников света для создания трехмерного изображения, Nvisage может распознавать более тонкие особенности лица. Более того, так как Nvisage генерирует трехмерную модель лица, ее можно вращать.

Более надежной разновидностью описываемого метода является идентификация по «тепловому портрету» лица или тела человека в инфракрасном диапазоне. Этот метод, в отличие от обычного, оптического, не зависит от изменений лица человека (например, появления бороды), так как тепловая картина лица меняется крайне редко.

Недавно появилось сообщение об устройствах Technology Recognition Systems (США), в которых происходит распознавание лица в инфракрасном свете. Данная технология основана на том, что термограмма лица человека (тепловая картинка, созданная излучением тепла кровеносными сосудами лица) уникальна для каждого человека и, следовательно, может быть использована в качестве биокода для систем контроля допуска (рис. 3.27). Данная термограмма является более стабильным кодом, чем геометрия лица, поскольку не зависит от времени и изменений внешности человека.

В процессе термографической идентификации личности индивидуальный рисунок распределения тепловых областей на лице человека вводится в компьютер с помощью инфракрасной камеры и платы захвата изображения, например, DT3152(PCI). Монохромное изображение, поступающее от инфракрасной видеокамеры, вводится в компьютер с помощью специального кабеля. В это же время к изображению добавляется специально созданная просмотровая таблица (look up table). Затем изображение подвергается обработке специальной утилитой, разработанной на C++. В это время и происходит идентификация по индивидуальному рисунку тепловых областей на лице.

Используя плату захвата изображения DT3152 и приложение для распознавания образов, компания Data Translation создала уникальную систему распознавания личности, отличающуюся высокой надежностью, скоростью, причем она доступна по стоимости.

Проблемы идентификации человека по лицу существенно упрощаются при переходе наблюдений в дальний инфракрасный диапазон световых волн. Предложено осуществлять термографию идентифицируемого лица, выявляющую уникальность распределения артерий на лице, снабжающих кожу теплой кровью. Проблема подсветки для этого класса биометрических устройств не существует, так как они воспринимают только температурные перепады лица и могут работать в полной темноте. На результаты идентификации не влияют перегрев лица, его переохлаждение, естественное старение личности, пластические операции, так как они не изменяют внутреннее расположение сосудов. Методу лицевой термографии доступно различение однояйцевых близнецов, кровеносные сосуды на их лицах имеют достаточно существенные различия. Дистанционное считывание с любого расстояния вне зависимости от освещенности обеспечивает высокую пропускную способность и вандалозащищенность. Метод рассчитан на использование специализированной видеокамеры дальнего инфракрасного диапазона, что и определяет его высокую стоимость.

Идентификация по глазу человека

В некоторых системах идентификации в качестве ключа используется глаз человека. Существует две разновидности этих систем, использующие разные идентификаторы. В первом случае в качестве «носителя» идентификационного кода применяется рисунок капилляров (кровеносных сосудов) на сетчатке (дне) глаза, а во втором — узор радужной оболочки глаза (рис. 3.28).

Для начала рассмотрим способ идентификации по узору кровеносных сосудов, расположенных на поверхности глазного дна (сетчатке). Сетчатка расположена глубоко внутри глаза, но это не останавливает современные технологии. Более того, именно благодаря этому свойству, сетчатка — один из наиболее стабильных физиологических признаков организма. Сканирование сетчатки происходит с использованием инфракрасного света низкой интенсивности, направленного через зрачок к кровеносным сосудам на задней стенке глаза. Для этих целей используется лазерный луч мягкого излучения. Вены и артерии, снабжающие глаз кровью, хорошо видны при подсветке глазного дна внешним источником света. Еще в 1935 году Саймон и Голдштейн доказали уникальность дерева кровеносных сосудов глазного дна для каждого конкретного индивидуума.

Сканеры для сетчатки глаза получили большое распространение в сверхсекретных системах контроля доступа, так как у них один из самых низких процентов отказа доступа зарегистрированных пользователей. Кроме того, в системах предусмотрена защита от муляжа.

В настоящее время широкому распространению этого метода препятствует ряд причин:

- высокая стоимость считывателя;
- невысокая пропускная способность;
- психологический фактор.

Невысокая пропускная способность связана с тем, что пользователь должен в течение нескольких секунд смотреть в окуляр на зеленую точку.

Рис. 3.28. Радужная оболочка и рисунок капиллярных сосудов на сетчатке человеческого глаза

С психологической точки зрения, многие отказываются смотреть в окуляр, когда им в глаз светит лазерный луч, несмотря на заверения медиков о безвредности процедуры.

Примером такого устройства распознавания свойств сетчатки глаза может служить продукция EyeDentify's — модель ICAM 2001 внешний вид которой представлен на рис. 3.29. Оно использует камеру с сенсорами, которые с короткого расстояния (менее 3 см) измеряют свойства сетчатки глаза. Пользователю достаточно взглянуть одним глазом в отверстие камеры ICAM 2001, и система принимает решение о праве доступа.

Основные характеристики считывателя ICAM 2001:

- время регистрации (enrolment) — менее 1 мин;
- время распознавания при сравнении с базой эталонов в 1 500 человек — менее 5 с;
- средняя пропускная способность — 4—7 с.

И тем не менее, эти системы совершенствуются и находят свое применение. В США, например, разработана новая система проверки пассажиров, основанная на сканировании сетчатки глаза. Специалисты утверждают, что теперь для проверки не нужно доставать из кармана бумажник с документами, достаточно лишь пройти перед камерой. Исследования сетчатки основываются на анализе более 500 характеристик. После сканирования код будет сохраняться в базе данных вместе с другой информацией о пассажире, и в последующем идентификация личности будет занимать всего несколько секунд. Использование подобной системы будет абсолютно добровольной процедурой для пассажиров.

Английская Национальная физическая лаборатория (National Physical Laboratory, NPL), по заказу организации Communications Electronics Security Group, специализирующейся на электронных средствах защиты систем связи, провела исследования различных биометрических технологий идентификации пользователей.

В ходе испытаний система распознавания пользователя по сетчатке глаза не разрешила допуск ни одному из более чем 2,7 млн «посторонних», а среди тех, кто имел права доступа, лишь 1,8% были ошибочно отвергнуты системой (проводилось три попытки доступа). Как сообщается, это был самый низкий коэффициент ошибочных решений среди проверяемых систем биометрической идентификации. А самый большой процент ошибок был у системы распознавания лица — в разных сериях испытаний она отвергла от 10 до 25% законных пользователей.

Еще одним уникальным для каждой личности статическим идентификатором является радужная оболочка глаза. Уникальность рисунка радужной оболочки обусловлена генотипом личности, и существенные отличия радужной оболочки наблюдаются даже у близнецов. Врачи используют рисунок и цвет радужной оболочки для диагностики заболеваний и выявления генетической предрасположенности к некоторым заболеваниям. Обнаружено, что при ряде заболеваний на радужной оболочке появляются характерные пигментные пятна и изменения цвета. Для ослабления влияния состояния здоровья на результаты идентификации личности в технических системах опознавания используются только черно-белые изображения высокого разрешения.

Идея распознавания на основе параметров радужной оболочки глаза появилась еще в 1950-х годах. Джон Даугман, профессор Кембриджского университета, изобрел технологию, в состав которой входила система распознавания по радужной оболочке, используемая сейчас в Nationwide ATM. В то время ученые доказали, что не существует двух человек с одинаковой радужной оболочкой глаза (более того, даже у одного человека радужные оболочки глаз отличаются), но программного обеспечения, способного выполнять поиск и устанавливать соответствие образцов и отсканированного изображения, тогда еще не было.

В 1991 году Даугман начал работу над алгоритмом распознавания параметров радужной оболочки глаза и в 1994 году получил патент на эту технологию. С этого момента ее лицензировали уже 22 компании, в том числе Sensar, British Telecom и японская OKI.

Получаемое при сканировании радужной оболочки глаза изображение обычно оказывается более информативным, чем оцифрованное в случае сканирования отпечатков пальцев.

Уникальность рисунка радужной оболочки глаза позволяет выпускать фирмам целый класс весьма надежных систем для биометрической идентификации личности. Для считывания узора радужной оболочки глаза применяется дистанционный способ снятия биометрической характеристики.

Системы этого класса, используя обычные видеокамеры, захватывают видеоизображение глаза на расстоянии до одного метра от видеокамеры, осуществляют автоматическое выделение зрачка и радужной оболочки. Пропускная способность таких систем очень высокая. Вероятность же ложных срабатываний небольшая. Кроме этого, предусмотрена защита от муляжа. Они воспринимают только глаз живого человека. Еще одно достоинство этого метода идентификации — высокая помехоустойчивость. На работоспособность системы не влияют очки, контактные линзы и солнечные блики.

Преимущество сканеров для радужной оболочки состоит в том, что они не требуют, чтобы пользователь сосредоточился на цели, потому что образец пятен на радужной оболочке находится на поверхности глаза. Даже у людей с ослабленным зрением, но с неповрежденной радужной оболочкой, все равно могут сканироваться и кодироваться идентифицирующие параметры. Даже если есть катаракта (повреждение хрусталика глаза, которое находится позади радужной оболочки), то и она никак не влияет на процесс сканирования радужной оболочки. Однако плохая фокусировка камеры, солнечный блик и другие трудности при распознавании приводят к ошибкам в 1% случаев.

В качестве такого устройства идентификации можно привести, например, электронную систему контроля доступа «Iris Access 3000», созданную компанией LG. Эта система за считанные секунды считывает рисунок оболочки, оцифровывает его, сравнивает с 4000 других записей, которые она способна хранить в своей памяти, и посылает соответствующий сигнал в систему безопасности, в которую она интегрирована. Система очень проста в эксплуатации, но при этом, данная технология обеспечивает высокую степень защищенности объекта.

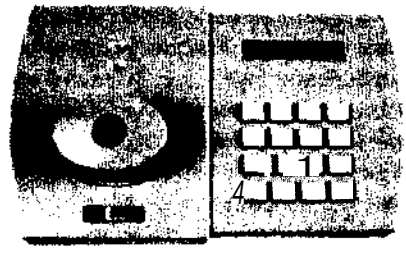


Рис. 3.29. Считыватель сетчатки глаза — модель ICAM 2001

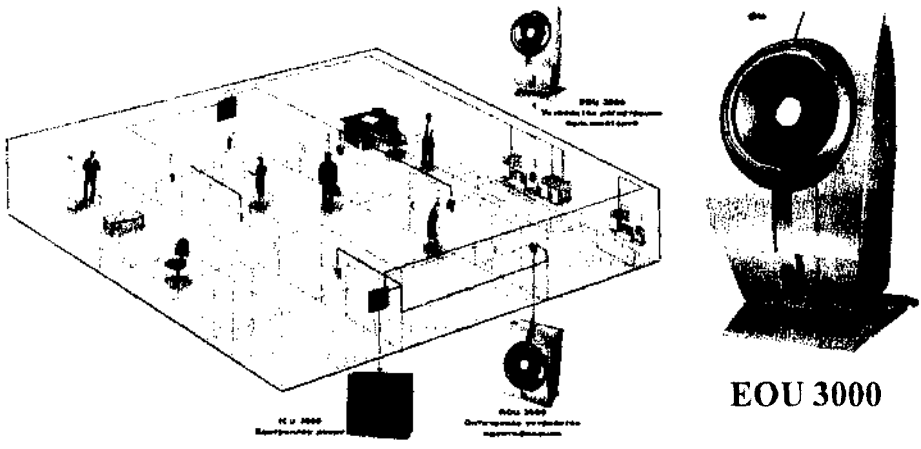


Рис. 3.30. Пример использования электронной системы распознавания «Iris Access 3000»

В состав системы входят:

- устройство регистрации пользователей EOU 3000;
- оптическое устройство идентификации / оптический считыватель ROU 3000;
- контроллер двери ICU 3000;
- сервер.

Устройство регистрации пользователей EOU 3000 обеспечивает начальный этап процесса регистрации пользователей. Оно снимает изображение радужной оболочки глаза при помощи камеры и подсветки. В процессе получения изображения и при его завершении устройство использует голосовую и световую подсказку.

Оптическое устройство идентификации, оно же оптический считыватель ROU 3000, содержит элементы для получения изображения радужной оболочки глаза. Голосовая и световая индикация информирует пользователя, определен он системой или нет.

Контроллер двери ICU 3000 создает специальный код (IrisCode) изображения сетчатки глаза, получаемой от считывателя ROU, сравнивает этот код с уже имеющимися в его памяти кодами изображений. При идентификации соответствующего кода, результат сообщается голосом из динамика в считывателе ROU 3000. К контроллеру возможно подключение до четырех считывателей ROD 3000, что обеспечивает управление четырьмя дверями.

Сервер выполнен на базе персонального компьютера. Он выполняет функции главного сервера, сервера, станции регистрации пользователей, станции мониторинга и управления системой. Главный сервер контролирует передачу информации из базы данных по запросу от одного сервера другим серверам. Сервер отвечает за управление рабочими станциями и контроллерами дверей ICU. Станция ввода изображения обеспечивает регистрацию пользователей при помощи устройства EOU 3000. Станция мониторинга производит отслеживание статуса контроллеров ICU, оптических считывателей ROU, устройства регистрации и состояния дверей ROU. Станция управления обеспечивает поддержку основной базы данных пользователей, загрузку необходимых данных в контроллер ICU.

Пример построения системы доступа на основе электронной системы распознавания радужной оболочки глаза «Iris Access 3000» представлен на рис. 3.30.

Перспективы распространения этого способа биометрической идентификации для организации доступа в компьютерных системах очень хорошие. Тем более, что сейчас уже существуют мультимедийные мониторы со встроенными в корпус видеокамерами. Поэтому на такой компьютер достаточно установить необходимое программное обеспечение, и система контроля доступа готова к работе. Понятно, что и ее стоимость при этом будет не очень высокой.

Далее мы рассмотрим, как используются поведенческие характеристики личности для ее идентификации.

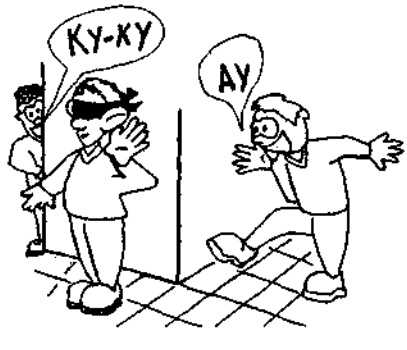
Идентификация по голосу

В современном мире все больше проявляется интерес к речевым технологиям, в частности, к идентификации личности по голосу. Это объясняется, с одной стороны, появлением высокопроизводительных вычислительных систем на базе персональных компьютеров и аппаратных средств, позволяющих производить ввод сигнала в компьютер, а, с другой стороны, высокой потребностью систем аутентификации в разных областях жизнедеятельности человека.

Метод опознавания личности по голосу существует с тех пор, как человек научился говорить. Поэтому достоинства и недостатки этого метода известны всем. Как не всегда по ответу на вопрос «Кто там?» мы можем определить, что за дверью стоит знакомый человек, и приходится развеивать свои сомнения, заглянув в дверной глазок, так и техническая система идентификации может ошибаться в силу изменения голоса отдельного человека.

Привлекательность данного метода — удобство в применении. Метод проверки голоса имеет два положительных отличия от остальных биометрических методов. Во-первых, это идеальный способ для телекоммуникационных приложений. Во-вторых, большинство современных компьютеров уже имеют необходимое аппаратное обеспечение. Продукты с проверкой голоса сейчас предлагают более 20 компаний.

Компания Keyware Technologies, например, поставляет OEM-производителям свой комплект программ для разработчиков VoiceGuardian. Уровень равной вероятности ошибки этой системы составляет 2—5% — это более низкая достоверность по сравнению с большинством остальных систем. Но данная технология хорошо подходит для верификации по голосу через коммутируемую телефонную сеть и она более надежна по сравнению с технологией частотного набора персонального идентификационного номера (PIN).



Основная проблема, связанная с этим биометрическим подходом, — точность идентификации. Однако это не является серьезной проблемой с того момента, как устройства идентификации личности по голосу различают характеристики человеческой речи. Голос формируется из комбинации физиологических и поведенческих факторов. В настоящее время идентификация по голосу используется для управления доступом

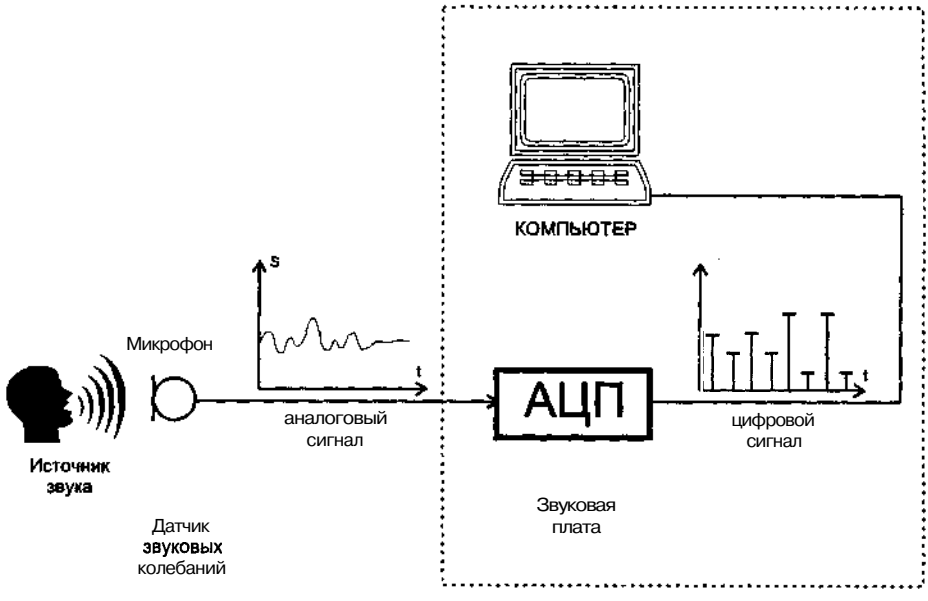


Рис. 3.31. Схема ввода речевых сообщений в компьютер

в помещение средней степени безопасности, например, лаборатории и компьютерные классы. Идентификация по голосу удобный, но в тоже время не такой надежный, как другие биометрические методы. Например, человек с простудой или ларингитом может испытывать трудности при использовании данных систем. Существует также возможность воспроизведения звукозаписи с магнитофона.

Технология распознавания голоса — вероятно, наиболее практичное решение для большинства сетевых приложений, во всяком случае, на данный момент. Системы распознавания голоса анализируют характеристики оцифрованной речи, в том числе ее тон, высоту и ритм.

Несмотря на остающиеся технические вопросы, в частности, на снижение надежности распознавания при наличии шумов, это весьма экономичное решение, так как микрофоны и звуковые карты уже давно получили прописку в сети. Схема ввода речевых сообщений в компьютер представлена на рис. 3.31.

Как известно, источником речевого сигнала служит речеобразующий тракт, который возбуждает звуковые волны в упругой воздушной среде. Сформированный речевой сигнал и передается в пространстве в виде звуковых волн. Приемник сигнала — это датчик звуковых колебаний. Обычно для этих целей используют микрофон — устройство для преобразования звуковых колебаний в электрические. Существует большое количество типов микрофонов (угольные, электродинамические, электростатические, пьезоэлектрические и др.). Но в микрофонах любого типа чувствительным элементом является упругая мембрана, посредством которой передается колебательный процесс под воздействием звуковых волн. Мембрана связана с элементом, который преобразует колебания мембраны в электрический сигнал.

С выхода микрофона сигнал подается на вход звуковой карты персонального компьютера. При записи звуковая карта представляет собой аналого-цифровой преобразователь с широкими возможностями настройки параметров оцифровки. Основными параметрами является частота дискретизации и разрядность кодирования. Данные параметры определяют качество и размер выборки, получаемой в результате записи. Причем размер записи и ее качество прямо пропорциональны, т. е. чем выше качество записи, тем больше ее размер.

Чтобы обеспечить компромисс между качеством и размером, воспользуемся знаниями о свойствах человеческого голоса при выборе параметров аналого-цифрового преобразования.

К настоящему моменту у нас и за рубежом реализованы системы автоматической идентификации по голосу, большинство из которых строятся по единой концептуальной схеме:

- производится регистрация пользователя и вычисляется шаблон;
- выбираются участки речевого потока для дальнейшего анализа;
- осуществляется первичная обработка сигнала;
- вычисляются первичные параметры;
- строится «отпечаток» (шаблон) голоса;
- производится сравнение «отпечатков» голосов и формируется решение по идентичности голосов или «близости» голоса к группе голосов.

Рассмотрим более подробно каждый из этапов.

На этапе регистрации новый пользователь вводит свой идентификатор, например, имя и фамилию, а затем произносит несколько раз ключевое слово или фразу (создаются эталоны). Число повторов ключевой фразы может варьироваться для каждого пользователя, а может быть постоянным для всех. После предварительной обработки фрагменты попарно сравниваются, и на основе их степени сходства вычисляется значение «отпечатка» (шаблона).

Для выбора фрагментов фонограммы, с целью извлечения необходимых параметров, существует несколько подходов. Например, часто применяют метод, в котором используется весь речевой сигнал за исключением пауз. Также существует метод выбора опорных сегментов — наиболее информативных участков речевого сигнала. При этом выбирают наиболее энергетически мощные звуки, т. к. они менее зависимы от шумов и искажений. В основном это гласные и звонкие согласные, произношение которых хорошо отражает работу голосовых связок и речевого тракта. Эти звуки обязательно имеют ярко выраженную неравномерность спектральной характеристики и именно в них выражена индивидуальная особенность мышечной активности речевого тракта личности.

Вероятность присутствия характерных индивидуальных особенностей голоса личности в 18 фонемах русского языка приведена в табл. 3.3, которая упорядочивает по информативности фонемы русского языка с позиций решения задачи идентификации личности. Фонема — это единица языка, с помощью которой различаются и отождествляются морфемы и тем самым слова (проще говоря — звуки). Наиболее информативны фонемы, расположенные в левой части таблицы. В правой части таблицы помещены фонемы, малоинформативные для целей идентификации личности, так как они позволяют узнавать диктора с вероятностью 0,5 и менее. Эти фонемы могут отражать особенности голоса личности только в сочетании с другими звуками.

Таблица 3.3. Вероятность распознавания личности по одной изолированной фонеме

Фонема	э	о	л	а	и	з	р	в	ж	м	г	у	ч	ц	х	с	ш	к
Вероятность	0,90	0,86	0,84	0,83	0,83	0,79	0,78	0,76	0,74	0,62	0,61	0,60	0,54	0,50	0,48	0,44	0,37	0,30

В процессе первичной обработки сигнала производится оценка спектральных параметров речи. Первые системы идентификации личности по особенности голоса строились исходя из частотных представлений и возможностей средств аналоговой фильтрации. В основу их работы положена различная тембральная окраска голосов и индивидуальная неравномерность распределения мощности произносимой фразы по частотному спектру. Базовыми процедурами для этого класса устройств являются узкополосная фильтрация сигнала и восстановление его огибающей. Например, подобная система фирмы Texas Instruments использует гребенку из 16-и узкополосных фильтров с шириной полосы 220 Гц, равномерно накрывающей частотный диапазон от 300 до 3000 Гц. Структура аналоговой части системы голосовой идентификации приведена на рис. 3.32.

При произношении контрольной фразы система идентификации осуществляет приведение сигнала к единому масштабу амплитуд за счет работы АРУ входного усилителя. Полосовые фильтры и детекторы огибающей их откликов позволяют получить 16 функций времени A1(t),A2(t),...,A16(t),характеризующих распределение энергии звукового сигнала по частотному спектру. Функция A0(t) описывает изменения значения энергии полного сигнала во всем диапазоне звуковых частот. При обучении система запоминает наиболее вероятные эталонные значения функций Ak(t) для конкретной личности и допустимые коридоры отклонений для этих функций.

Первичные параметры речевого сигнала должны обладать следующими свойствами:

- отражать индивидуальность диктора;
- быть легко и надежно выделяемы из сигнала;
- мало зависеть от мешающих факторов;
- быть инвариантными к эмоциональному и физическому состоянию диктора;
- слабо поддаваться имитации.

В качестве первичных параметров обычно используются такие характеристики речевого сигнала, как АЧХ, основной тон, форманты, расстояние между обертонами, формы импульсов возбуждения, длительность отдельных звуков и т. п.

Как правило, при произнесении парольной фразы длительности составляющих ее звуков и пауз между ними могут варьироваться в пределах от 10 до 50%. Для компенсации временной нестабильности произнесения диктором парольных фраз можно использовать два способа:

- подгонка под эталон путем сжатия и растяжения участков, соответствующих отдельным звукам, средствами динамического программирования;
- выделение центра звуковой области и идентификационные измерения в окрестностях центральной части фонемы, тогда абсолютные значения длительностей фонем и пауз между ними не играют существенной роли.

По полученным на предыдущем этапе параметрам, исходя из выбранной математической модели, строится «отпечаток» голоса. Далее производится сравнительный анализ отпечатков голосов. Анализировать можно различными способами, начиная от

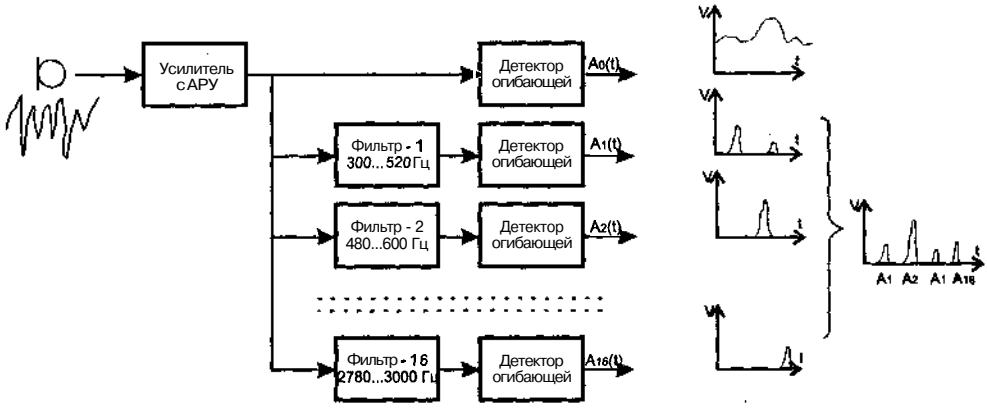


Рис. 3.32. Идентификация голоса многоканальным анализом

простых статистических методов и заканчивая тем, что решение принимается нейросетью и/или сложной системой искусственного интеллекта.

Задача идентификации возникает тогда, когда необходимо найти ближайший голос (или несколько голосов) из фонотеки к рассматриваемой фонограмме. Необходимость автоматизации этой задачи напрямую зависит от количества голосов в фонотеке, уровня эксперта и необходимой оперативности принятия решения.

Обычно после задачи идентификации приходится решать вторую задачу, в которой подтверждается или опровергается принадлежность фонограммы конкретному голосу, т. е. задачу верификации.

Решение задачи идентификации позволяет решать задачу верификации не на всей фонотеке, а только на группе ближайших голосов, что значительно сокращает время обработки фонограммы.

Описанный выше частотный подход к идентификации личности мог быть реализован средствами аналоговой фильтрации уже 30—40 лет назад и именно по этой причине в то время произошел всплеск интереса к этому классу систем голосовой идентификации. По мере развития средств вычислительной техники и методов цифровой фильтрации, интерес к частотным методам идентификации замещается на интерес к системам, применяющим линейные предсказатели речевого сигнала. Системы идентификации с линейным предсказанием речи используют описание сигнала во временной области. Пример описания во временной области парольной фразы «ПАРОЛЬ» приведен на рис. 3.33.

В основу кодирования речи методом линейного предсказания положена волновая структура речевого сигнала, особенно хорошо наблюдаемая при произношении гласных. На рис. 3.33 выделен фрагмент парольной фразы, соответствующий гласной «О» и состоящий из последовательности затухающих волн, возбуждаемых говорящим с периодом основного тона. Соседние волны волновой пачки достаточно похожи друг на друга. Метод линейного предсказания построен на аппроксимации соседних волн в звуковой пачке переходным процессом некоторого линейного цифрового фильтра.

При описании звукового сигнала методом линейного предсказания исходный сигнал разбивают на отдельные интервалы анализа фиксированной длины (обычно длина интервала анализа составляет 20 мс.). Далее определяют тип звука внутри интервала

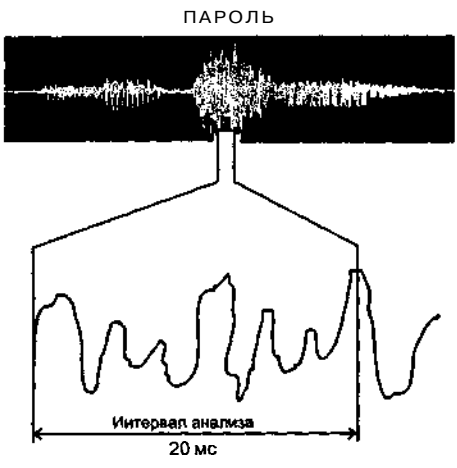


Рис. 3.33. Структура *речевого* сигнала парольной фразы

анализа (шум или тональный звук). Если внутри интервала находится шумовой участок, тогда определяют только его энергетические параметры. Если внутри интервала анализа присутствует тональный фрагмент, то сигнал дополнительно описывают путем задания коэффициентов линейного предсказателя (линейного цифрового фильтра) и задания периода импульсов основного тона, возбуждающих переходные процессы на выходе линейного предсказателя.

В качестве недостатка биометрических систем идентификации личности по голосу необходимо отметить, прежде всего, то, что парольную фразу трудно сохранить в тайне. Современные средства акустического прослушивания (радиожучки и другие подслушивающие устройства) позволяют достаточно успешно осуществлять несанкционированное копирование парольной фразы. Ожидается, что исключение опасности использования злоумышленниками «магнитофонов» произойдет при переходе к идентификации личности на произвольных фразах. Как потенциальное противодействие «магнитофонам» используют случайный розыгрыш парольных фраз, а также комбинирование с другими методами биометрической аутентификации.

Методы голосовой идентификации применяют и на практике. Технология верификации говорящего компании Veri Voice обеспечивает доступ к закрытым страницам Web с удаленного компьютера; удаленный доступ посредством идентификации голоса и Remote Access Server (RAS) компании Microsoft, двухуровневую идентификацию с помощью верификации голоса и смарт-карт при доступе к локальным и удаленным приложениям. Для регистрации система «просит» пользователя произнести пароль — последовательность случайных цифр. Голосовой отпечаток занимает обычно от 2 до 5 кбайт, а фраза-пароль длится около двух секунд звучания.

Подпись

Подпись — это традиционный способ подтверждения документов, банковских операций. Большинство из нас получали когда-нибудь деньги в банке или сберкассе, где они и познакомились с этим методом идентификации личности. Вспомните, что банковские служащие сверяют вашу подпись с образцом на глаз и достаточно часто, особенно при выдаче крупных сумм, просят расписаться по несколько раз. Известны даже случаи, когда получатели не могли получить деньги вследствие изменения у них почерка или самой подписи.

Подпись является таким же уникальным атрибутом человека, как и другие его биохарактеристики. Человеческий почерк непостоянен, поэтому распознавание подписи вызывает сомнение как средство автоматической идентификации личности в больших открытых системах. В общем, считается, что существование крайне нестабильных и легко имитируемых подписей — одна из основных причин снижения производительности системы, распознающей подпись человека. Но, с другой стороны, подпись — это привыч-

ный для нас метод идентификации, и он, в отличие от отпечатка пальца, не ассоциируется у нас с криминальной сферой.

Рис. 3.34. Образцы подписи одного и того же человека, сделанные в разное время

Конечно же применять этот метод можно далеко не везде, но использовать его в банковской сфере или для входа в компьютерную сеть можно. В этих случаях проверка правильности подписи может стать наиболее эффективным, а, главное, необременительным и незаметным способом идентификации.

Любая рукопись в своеобразии начертания букв доносит до нас что-то личностное. Графологи, рассматривая частокол черточек и завитушек, много могут рассказать об их авторе. Они не только убедительно демонстрируют методы определения пола, возраста, образования, рода занятий писавшего, но и достаточное внимание уделяют экспериментальным основаниям этого научного направления. В классификации Зуева-Инсарова — автора фундаментальных работ по графологии — например, содержатся такие формальные признаки почерка, как:

- сила нажима;
- динамичность и напряженность движения;
- вытянутость, наклон и степень связанности букв;
- направление строки;
- расположение и содержательность текста;
- способ держания орудия письма;
- равномерность и соразмерность букв и слов;
- ритм и выразительность письма.

А что можно узнать с помощью компьютера о человеке? Попробуем поискать аналогии. Компьютерная система тоже учитывает несколько параметров почерка: саму форму начертания, динамику движения пера (угол наклона, скорость и ускорение), степень нажима. С помощью этих параметров можно распознать личность с достаточно высокой вероятностью. При этом все перечисленные характеристики пользователя напрямую зависят от его психоэмоционального состояния, поэтому идентификация в некоторых случаях может быть затруднена. На рис. 3.34 представлены образцы подписи одного и того же человека, сделанные в разное время.

Устройства идентификации подписи используют, в основном, специальные ручки, чувствительные к давлению столы, или комбинацию обоих. Устройства, использующие специальные ручки, менее дороги и занимают меньше места, но в то же время срок их службы короче.

Существует два способа обработки данных о подписи:

- метод простого сравнения с образцом;
- метод динамической верификации.

Метод простого сравнения с образцом очень ненадежен, т. к. основан на обычном сравнении введенной подписи с хранящимися в базе данных графическими образцами. По причине того, что подпись не может быть всегда одинаковой, процент ошибок этого метода достаточно высок. Хорошо подделанная подпись вполне может удовлетворить систему опознавания.

Математический аппарат метода динамической верификации намного сложнее. Он позволяет фиксировать параметры процесса подписи в реальном времени, например, скорость движения руки на разных участках, порядок нанесения штрихов, форму и направление штрихов, силу давления и длительность различных этапов подписи. Это гарантирует, что подпись не подделает даже опытный графолог, поскольку никто не может в точности скопировать поведение руки владельца подписи.

Процесс верификации подписи происходит в несколько этапов. Например, Signature Series компании РепОр позволяет просматривать, снимать и ставить письменные цифровые подписи на электронные документы.

Подписи РепОр делятся на два типа. Реальную подпись пользователь ставит с помощью ручки и устройства ввода, после чего подпись анализирует программное обеспечение с целью проверки личности. Затем программа подписывает документ. В случае удостоверяющего штампа пользователь вводит пароль (это можно сделать посредством произнесения пароля или сканирования отпечатков пальцев) для авторизации штампа. Затем этот штамп на основе заранее снятой подписи прикрепляется к документу.

Регистрирует и проверяет подписи инструментарий хранения и администрирования РепОр Signature Book.

Наконец, в соответствии с тенденцией распространения технологий идентификации на мобильные устройства программное обеспечение РепОр PocketSign позволяет вводить подпись пользователя через устройства Palm Computing, когда требуется интерактивно подписать форму.

Продукция Biometric Signature Verification компании Cyber-SIGN составляет основу ее технологии верификации подписи. Предложение Cyber-SIGN включает клиентское и серверное программное обеспечение, а также графический планшет для каждого клиентского места.

Пользователь предоставляет исходную подпись, на основе которой составляется шаблон, хранимый в базе данных или на защищенном сервере Cyber-SIGN. Зашифрованные образы последующих подписей сравниваются с защищенным шаблоном на сервере. Программное обеспечение способно также выявлять и распознавать изменения в подписи с течением времени.

Для идентификации пользователей используется и «интеллектуальное перо» (SmartPen) — действительно пишущая шариковая ручка, снабженная сенсорами и крошечным радиопередатчиком, выпускаемая компанией LCI Computer Group (Дания). Ее важное достоинство в том, что она может писать и на обычной бумаге. Пользователь, к примеру, ставит свою подпись, а ручка снимает детальные динамические биометрические показатели, набор которых уникален для каждого человека, и передает их в компьютер. На головном компьютере может храниться база данных с «профилями рук» множества пользователей. В процессе письма на плоской поверхности ручка движется в трехмерном пространстве. В третьем измерении, в котором ручка давит на бумагу, фиксируются микроперемещения.

В действительности, комплект оборудования SmartPen — это весьма сложный технический комплекс. Ручка содержит микромышь, снабженную датчиками для снятия параметров трехмерной траектории, сигнальный процессор для обработки полученных данных, приемопередатчик и даже систему криптографической защиты, чтобы предотвратить перехват данных, передаваемых по радиоканалу.

Клавиатурный почерк

Все люди воспринимают происходящие события по-разному. Попробуйте за короткое время прикинуть количество точек или гласных букв в длинных словах, размеры горизонтальных и вертикальных линий, — сколько будет испытуемых, столько и мнений. Эти особенности человеческой психики также подходят для идентификации. Правда, в зависимости от состояния и самочувствия человека полученные значения будут «плавать», поэтому на практике полагаются на интегральный подход, когда итог подводится по нескольким проверкам, учитывая и работу с клавиатурой. Например, способ идентификации может быть таким: на экране, на несколько секунд, появляются вертикальные или горизонтальные линии. Их размер и количество случайны. Пользователь набирает соответствующие, на его взгляд, цифры. Таким образом, выясняются: характеристики клавиатурного почерка, оценивается, насколько указанные длина и число линий близки к действительности, внимание и точность подсчета (насколько длина одной линии правильно сопоставлена с соседней). И, наконец, результаты сравниваются с эталоном. В этом методе не так важны ошибки в определении размеров, главное — чтобы они повторялись и при настройке, и при идентификации.

С точки зрения использования скрытого мониторинга компьютерных систем безопасности представляет интерес классификация психофизических параметров пользователя, к которым относятся: клавиатурный почерк, подпись мышью, реакция на события, происходящие на экране. Мы же остановимся только на рассмотрении использования клавиатурного почерка для идентификации личности.

Одна из достаточно сложных задач, повседневно решаемых многими людьми, — быстрый набор текстов с клавиатуры компьютера. Обычно быстрого клавиатурного ввода информации удается достичь за счет использования всех пальцев обеих рук. При этом у каждого человека проявляется свой уникальный клавиатурный почерк. Клавиатурный почерк — это набор динамических характеристик работы на клавиатуре.

Не многие догадываются, что в общении с компьютером индивидуальность пользователя проявляется в скорости набора символов, привычки использовать основную или дополнительную часть клавиатуры, характере «сдвоенных» и «строенных» нажатий клавиш, в излюбленных приемах управления компьютером и т. д. И в этом нет ничего удивительного — это сродни способности меломанов различать на слух пианистов, исполняющих одно и то же произведение, или работе телеграфистов, использующих код Морзе.

Этот способ идентификации популярен в США для предотвращения доступа детей в Internet через домашние компьютеры. Даже если ребенок подсмотрел или узнал пароль родителей, то он не сможет им воспользоваться. Также этот метод можно использовать для дополнительной защиты при организации доступа в компьютерных системах.

Опознавание клавиатурного почерка состоит в выборе соответствующего эталона из списка хранимых в памяти компьютера эталонов, на основе оценки степени близости этому эталону параметров почерка одного из операторов, имеющих право на работу с данным компьютером. Решение задачи опознавания пользователя сводится к решению задачи распознавания образов.

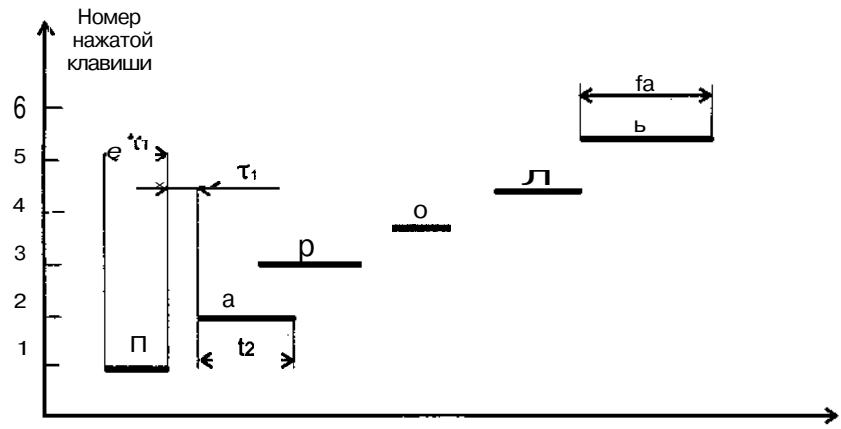


Рис. 3.35. Сбор биометрической информации о работе пользователя

Классический статистический подход к распознаванию пользователя по клавиатурному почерку (набор ключевых слов) выявил ряд интересных особенностей: зависимость почерка от буквенных сочетаний в слове, существование глубоких связей между набором отдельных символов, наличие «задержек» при вводе символов.

Весьма важной характеристикой биометрической идентификации является и длина парольной фразы. Практика показывает, что парольная фраза должна быть легко запоминающейся и содержать от 21 до 42 нажатий на клавиши. При синтезе парольной фразы допустимо использование слов со смыслом.

Кроме того, здесь возможен анализ таких признаков, как зависимость скорости ввода слов от их смысла, относительное время нажатия различных клавиш и др. Причем они в некоторых случаях даже более информативны: например, реакция тестируемого на различные термины укажет сферу его интересов. Действительно, химик быстрее наберет «водород», «соединение», чем «программа» или «экскаватор». А модельеру будут привычнее такие слова, как «манекен» или «выкройка».

Сбор биометрической информации о работе пользователя (рис. 3.35) при анализе клавиатурного почерка происходит при помощи замеров интервалов между нажатиями клавиш и времени их удержаний, после чего полученные результаты формируются в матрицу межсимвольных интервалов и вектор времен удержаний клавиш. После сбора биометрической информации полученные данные сравниваются со своими эталонными значениями.

Как же можно выявить индивидуальные особенности клавиатурного почерка? Да так же, как и при графологической экспертизе: нужны эталонный и исследуемый образцы текста. Лучше, если их содержание будет одинаковым — так называемая парольная или ключевая фраза. Разумеется, по двум-трем, даже по десяти нажатым клавишам отличить пользователя невозможно. Нужна статистика.

При наборе ключевой фразы компьютер позволяет зафиксировать много различных параметров, но для идентификации наиболее удобно использовать время, затраченное на ввод отдельных символов. Из рис. 3.35 видно, что времена нажатий клавиш t1, t2,....tn различны и, соответственно, значения этих параметров можно употреблять

для выявления характерных особенностей клавиатурного почерка пользователя. Кроме того, можно использовать как контролируемые параметры интервалы между нажатием соседних клавиш. Контролируемые параметры существенно зависят от того, сколько пальцев использует при наборе пользователь, от характерных для пользователя сочетаний движений различных пальцев руки и от характерных движений рук при наборе. Например, если заставить пользователя работать одним пальцем одной руки, то клавиатурный почерк практически полностью теряет свою индивидуальность. В этом случае времена нажатия клавиш перестают отражать индивидуальность людей, т. к. интервалы между нажатиями становятся пропорциональны расстоянию между клавишами, а перекрытие нажатий соседних клавиш становится невозможным.

Уникальные особенности клавиатурного почерка выявляются двумя методами:

- по набору ключевой фразы;
- по набору «свободного» текста.

Каждый из них обязательно имеет режимы настройки и идентификации. При настройке определяются и запоминаются эталонные характеристики ввода пользователем ключевых фраз, например, время, затраченное на отдельные символы. А в режиме идентификации эталонное и полученное множества сопоставляются после исключения грубых ошибок.

Набор «свободного» текста производится по самым разнообразным фразам (ключевая фраза, как правило, одна и та же), что имеет свои преимущества, позволяя получать индивидуальные характеристики незаметно, не акцентируя внимание пользователя на парольной фразе.

Выбор схемы проверки зависит от приложения, с которым она используется. Например, если бухгалтер захотел получить коротенькую справку, а компьютер вместо этого предлагает набрать 2—3 странички «свободного» текста, чтобы убедиться, что перед ним действительно нужное лицо. Тут никаких нервов не хватит и это вызовет только раздражение, а как следствие — пользователь будет всячески стараться избегать такой системы идентификации.

С другой стороны, тот, кто имеет допуск к секретам, может работать с такой программой целый день, время от времени отлучаясь от компьютера. А чтобы в этот момент злоумышленники не воспользовались раскрытой системой, желательно периодически проводить «негласную проверку». Такие системы позволяют постоянно контролировать, законный ли пользователь сидит за компьютером.

Нужно отметить, что при использовании этих методов появляется возможность не только подтвердить подлинность, но и проанализировать его состояние. Описанный подход к защите от несанкционированного доступа позволяет:

- G контролировать физическое состояние сотрудников;
- покончить с практикой нарушения правил безопасности при работе с паролями;
- обеспечить более простой и такой же надежный метод входа в сеть.

Методы и средства защиты информации от вредоносного программного обеспечения

При работе в сети Internet персональный компьютер подвергается постоянной опасности заражения компьютерными вирусами при получении как исполняемых (программных), так и документальных файлов. Особенно это опасно, если компьютер является рабочей станцией компьютерной сети. В этих условиях ущерб, нанесенный вредоносным программным обеспечением, может быть максимальным. С программными файлами можно получить загрузочные, полиморфные, шифрованные стелс-вирусы, с офисными документами возможно получение различных макровирусов.

Современный хакерский инструментарий настолько автоматизирован, что даже люди, не очень сведущие в сетевых и коммуникационных технологиях, могут без труда воспользоваться ими. В результате сетевые администраторы проявляют интерес к любым системам обеспечения информационной безопасности, которые попадают в их поле зрения.

Корпоративная сеть сегодня — настоящее богатство для любой компании, а ее администратор волей-неволей становится своего рода щитом, защищающим неприкосновенность этого богатства. Какие же меры позволяют повысить безопасность охраняемой территории? Конечно же, использование специального программного обеспечения, предназначенного для защиты компьютеров и сетей от вирусов, программных закладок, «дыр» и т. д.

Сегодня на рынке уже присутствуют изощренные средства обнаружения незваных гостей, стремящихся незаконно проникнуть в ваши сетевые владения. Однако такие средства нельзя воспринимать как законченные решения в области информационной безопасности. Они скорее являются еще одним интеллектуальным инструментом, помогающим реализовать стратегию защиты корпоративной сети наряду с другими компонентами вроде антивирусных приложений. В частности, система обнаружения сетевых атак позволяет провести мониторинг сетевой активности и выявить наиболее уязвимые места в сети или на отдельных хост-компьютерах. Более того, разные продукты данной категории неэквивалентны по функциональным возможностям. Вот почему крупные компании, серьезно беспокоящиеся о защите своих коммуникационных и информационных ресурсов, устанавливают сразу несколько детектирующих систем. Но наличие уже одного подобного продукта заметно повышает степень защищенности вашей организации по сравнению с той, которая была до начала его использования.

При существующем многообразии вирусов и их мутаций предотвратить заражение может только полнофункциональная антивирусная система, имеющая в своем арсенале все известные технологии борьбы с «инфекционными болезнями»: не только сканер-полифаг, но и резидентный on-line-монитор, средства контроля программной целостности (CRC) и эвристического поиска вирусных сигнатур.

Каждый новый вирус необходимо обнаружить как можно быстрее (а некоторые вирусы намеренно долго себя не проявляют, чтобы у них было достаточно времени на распространение). Проблема в том, что нет четкого способа определить заранее, что при своем выполнении данная программа проявит вирусоподобное поведение. Как нет единого лекарства от всех болезней, так нет универсальной «вакцины» от всех видов

вредоносного программного обеспечения. На все 100% защититься от вирусов практически невозможно (подразумевается, что пользователь меняется дискетами с друзьями и играет в игры, а также получает информацию из других источников, например из сетей). Если же не вносить информацию в компьютер извне (изолированный компьютер), заразить его вирусом невозможно — сам он не родится. Но в наше время это достаточно сложно. Поэтому, чтобы сталкиваться с вирусами как можно реже или, по крайней мере, только сталкиваться, не допуская их на жесткий диск своего винчестера, нужно соблюдать самые элементарные правила «компьютерной гигиены»: проверка дискет, содержимого CD-дисков на наличие вирусов самыми надежными антивирусными и постоянно обновляемыми программами.

В отличие от одиночного пользователя, проблема, которую решают специалисты, отвечающие за обеспечение антивирусной безопасности в крупных организациях, на самый поверхностный взгляд выглядит следующим образом: обеспечить максимальную антивирусную защиту при минимальных затратах. Ну а если взглянуть внимательнее, то открывается громадный перечень практических, экономических и организационных вопросов, которые рано или поздно встают перед специалистом. Такими стратегическими вопросами являются:

- что дешевле: предотвратить заражение или лечить?
- как оценить допустимые затраты на обеспечение антивирусной безопасности?
- что является объектом защиты?
- какова требуемая степень защищенности?
- как организовать защиту?

В настоящее время уровень экономически допустимых затрат на приобретение и внедрение антивирусной системы оценивается в размере 5—10% от потенциальных потерь от вирусной атаки.

Риск появления в системе какой-нибудь пакости возрастает с каждым днем. На самом деле важно не количество различных вирусов, а степень их распространения. Вирус, обнаруженный где-то далеко, в одной-единственной компании, вряд ли заставит сетевых менеджеров не спать по ночам. Совсем иное дело те программы, которые распространяются через Internet. Когда в мае 2000 года появился вирус LoveLetter, в течение одного месяца было выявлено более 23 тыс. заражений этим вирусом. А уже в декабре их число превысило 100 тыс.

Согласно отчетам компании Trend Micro, корпоративные пользователи постоянно сталкиваются с фактами проникновения вирусов в свои сети (табл. 3.4).

Приведем некоторые описания вирусов, которые нанесли наиболее существенный ущерб корпоративным заказчикам в последнее время.

Вирус, который был недавно обнаружен несколькими пользователями Internet, — PE_FUNLOVE.4099 — это далеко не новый резидентный вирус под Windows. Он инфицирует файлы как на локальных дисках, так и на дисках, доступных по сети. При запуске инфицированного файла вирус PE_FUNLOVE.4099 записывает файл FLCSS.EXE в системный каталог Windows и пытается заразить все файлы с расширениями EXE, OCX и SCR. На системах Windows NT вирус PE_FUNLOVE.4099 пытает-

Таблица 3.4. Вирусы, которые тревожат корпоративных пользователей

10 наиболее распространенных вирусов «In-the-Wild»	10 вирусов, которые наиболее тревожат корпоративных пользователей	10 наиболее распространенных вирусов на начало 2001 года
TROJ_MTX.A	VBS_KAKWORM.A	VBS_KAKWORM.A
TROJ_HYBRIS.B	TROJ_MTX.A	TROJ_PRETTY_PARK
VBS_KAKWORM.A	JOKE_WOW	TROJ_SKA
TROJ_HYBRIS.A	W97M_ASSILEM.B (Melissa)	VBS_LOVELETTER
TROJ_BYMER	TROJ_HYBRIS.B	PE_CIH
TROJ_NAVIDAD.E	JOKE_BURPER	W97M_MELISSA
TR0J_PRETTY_PARK	TROJ_BYMER	TROJ_MTX.A
TROJ_CLICK	VBS_LOVELETTER	TROJ_QAZ.A
TROJ_HYBRIS.D	W97M_THUS	W97M_ETHAN.A
TROJ_SUB7.BONUS	TROJ_PRETTY_PARK	097M_TRISTATE

ся изменить файлы NTLDR и NTOSKRNL.EXE с целью дать всем пользователям права администратора. Это происходит после перезагрузки системы после того, как пользователь с правами администратора зайдет в систему.

Новый вирус TROJ_NAVIDAD.E — это вариант вируса TROJ_NAVIDAD.A, который был впервые обнаружен в ноябре 2000 года. Оригинальный TROJ_NAVIDAD.A содержит ошибку, приводящую к тому, что при запуске EXE-файла выводится сообщение об ошибке. В новом вирусе этот недостаток исправлен, и он корректно инсталлируется в системе, после чего рассылает себя по адресам из адресной книги инфицированного пользователя в виде присоединенного файла EMANUEL.EXE. Несмотря на то что TROJ_NAVIDAD.E был обнаружен в декабре 2000 года, он продолжает распространяться.

Деструктивный вирус PE_KRIZ.4050, обнаруженный in-the-wild, — это старый 32-битный вирус под Windows, снова был недавно обнаружен во многих странах. Так же как несколько других старых вирусов, PE_KRIZ.4050 смог вернуться, так как был выпущен по ошибке в патче к компьютерной игре. Вирус PE_KRIZ.4050 содержит деструктивную функцию, сходную с функцией вируса PE_C1H, которая позволяет ему изменять данные в CMOS и обнулять BIOS.

Новое семейство червей — VBSJFUNNY, написанных на Visual Basic Script, было недавно обнаружено в Европе. При запуске эти черви ищут определенный ключ в реестре, и если его нет, то они рассылают по почте сообщения по всем адресам из адресной книги Microsoft Outlook с присоединенным к ним вирусом. Если указанный ключ найден, то черви записывают на диск исполняемый файл (STARTX.EXE), который является известным троянцем, похищающим пароли.

Вирус VBS_COLOMBIA — это новая модификация вируса VBS_LOVELETTER.A, имеющего деструктивную функцию, нацеленную на файлы с расширениями VBS, VBE, .JSE, CSS, WSH, SCT, .HTA, JPG, JPEG, MP3 и MP2.

Учитывая разнообразие вредоносных программ, приходится прибегать к различным стратегиям для защиты сети от коварного и вероломного кода.

Целью антивирусной стратегии является эффективное предотвращение заражения вирусами информационной системы. Другими словами, не максимально быстрое обнаружение и удаление появляющихся вирусов, а создание условий, при которых уже само появление вируса на пользовательском компьютере или, еще хуже, на сервере будет рассматриваться как чрезвычайное происшествие. Поэтому в основе всей стратегии антивирусной безопасности любой фирмы должны лежать следующие разделы:

- политика антивирусной безопасности;
- план работ по обеспечению антивирусной безопасности;
- порядок действий в критических ситуациях.

Разумеется, каждая фирма работает с различным уровнем информационной безопасности и в разных условиях информационной среды. То, что совершенно неприемлемо, например, для банка (использование сотрудниками дискет, принесенных из дома), может являться нормой работы в редакции газеты или в агентстве новостей. Поэтому все элементы стратегии организации должны полностью соответствовать целям и задачам, решаемым ее информационной системой, и специфике тех условий, в которых она работает. Следовательно, и приобретаемая антивирусная система должна полностью отвечать требованиям принятой стратегии.

Антивирусное программное обеспечение

Начнем рассмотрение материала данного раздела со знакомства с принципами построения антивирусного программного обеспечения. Многие считают, что антивирусная программа — это противоядие от всех болезней и, запустив антивирусную программу или монитор, можно быть абсолютно уверенным в их надежности. Такая точка зрения в корне неверна. Дело в том, что антивирус — тоже программа, пусть даже написанная профессионалом высокого класса. Но эта программа способна распознавать и уничтожать только известные вирусы. Иными словами, антивирус против конкретного вируса можно написать только в том случае, когда у программиста есть хотя бы один экземпляр этого вируса.

Поэтому между авторами вирусов и антивирусов идет бесконечная «война». И хотя создателей вирусов гораздо больше, но у их противников есть преимущество! Дело в том, что существует большое количество вирусов, алгоритм которых практически скопирован с алгоритма других вирусов. Как правило, такие вариации создают непрофессиональные программисты, которые по каким-то причинам решили написать вирус. Для борьбы с такими «копиями» придумано новое оружие — эвристические анализаторы. С их помощью антивирус способен находить подобные аналоги известных вирусов, сообщая пользователю, что на его компьютере, похоже, завелся вирус. Естественно, надежность эвристического анализатора не 100%, но все же его коэффициент полезного действия больше 0,5. Таким образом, в этой информационной войне, как, впрочем, и в любой другой выжи-

вают сильнейшие. Вирусы, которые не распознаются антивирусными детекторами, способны написать только опытные и высококвалифицированные программисты.

Для организации эффективной антивирусной защиты необходимо наличие соответствующего антивирусного средства. Несмотря на все разнообразие современных антивирусных программных продуктов, принципы их работы одинаковы. К основным функциям современных антивирусов относятся:

- сканирование памяти и содержимого дисков по расписанию;
- сканирование памяти компьютера, а также записываемых и читаемых файлов в реальном режиме времени с помощью резидентного модуля;
- выборочное сканирование файлов с измененными атрибутами (размером, датой модификации, контрольной суммой и т. д.);
- сканирование архивных файлов;
- распознавание поведения, характерного для компьютерных вирусов;
- удаленная установка, настройка и администрирование антивирусных программ с консоли системного администратора; оповещение системного администратора о событиях, связанных с вирусными атаками, по электронной почте, пейджеру и т. д.;
- принудительная проверка подключенных к корпоративной сети компьютеров, инициируемая системным администратором;
- удаленное обновление антивирусного программного обеспечения и баз данных с информацией о вирусах, в том числе автоматическое обновление баз данных по вирусам посредством Internet;
- фильтрация трафика Internet на предмет выявления вирусов в программах и документах, передаваемых посредством протоколов SMTP, FTP, HTTP;
- выявление потенциально опасных Java-апплетов и модулей ActiveX;
- функционирование на различных серверных и клиентских платформах, а также в гетерогенных корпоративных сетях;
- ведение протоколов, содержащих информацию о событиях, касающихся антивирусной защиты.

В связи с тем, что одной из основных характеристик современных вирусных атак является их высокая скорость распространения и высокая частота появления новых атак, современное антивирусное программное обеспечение нужно обновлять как можно чаще, тем самым повышая качество защиты. Необходимо учитывать все актуальные на текущий момент времени вирусные угрозы. Но наличие антивирусного программного обеспечения — это обязательное, но не достаточное условие для отражения вирусной атаки. Мало иметь в своем распоряжении средство, следует продумать и методы его правильного использования. Защита от вирусов должна быть элементом политики безопасности, которую понимают и соблюдают все пользователи системы.

В настоящее время обычная корпоративная компьютерная сеть отечественного заказчика включает в себя десятки и сотни рабочих станций, десятки серверов, разнообразное активное и пассивное телекоммуникационное оборудование и, как правило, имеет очень сложную структуру (рис. 36).

Стоимость обслуживания такой сети катастрофически растет вместе с ростом числа подключенных рабочих станций. Сейчас все только и говорят о том, как в данных условиях можно уменьшить совокупную стоимость владения или эксплуатации компьютерной инфраструктуры предприятия. Очевидно, что расходы на антивирусную

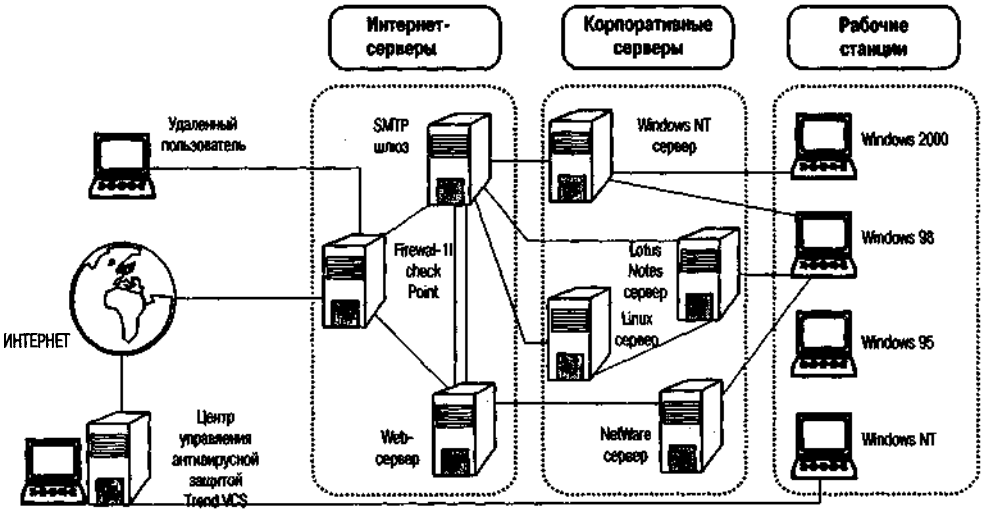


Рис. 3.36. Типовая архитектура корпоративной сети

защиту корпоративной сети здесь являются не последним пунктом в списке общих расходов предприятия. Однако существует принципиальная возможность оптимизации и снижения этих расходов путем использования специальных решений, позволяющих централизованно управлять антивирусной защитой корпоративной сети в реальном масштабе времени. Необходимо, чтобы такие решения позволяли администраторам сети предприятия отслеживать все точки проникновения вирусов с единой консоли управления и согласно технологии «клиент-сервер» эффективно управлять всеми присутствующими в корпоративной сети антивирусными средствами различных производителей.

Такая стратегия антивирусной защиты позволяет блокировать все возможные точки проникновения вирусов, такие как:

- проникновение вирусов на рабочие станции при использовании на рабочей станции инфицированных файлов с переносимых источников (флоппи-диски, компакт-диски, Zip, Jazz, Floptical и т. д.);
- заражение вирусами с помощью бесплатного инфицированного программного обеспечения, полученного из Internet через Web или FTP и сохраненного на локальной рабочей станции;
- проникновение вирусов при подключении к корпоративной сети инфицированных рабочих станций удаленных или мобильных пользователей;
- заражение вирусами с удаленного сервера, подсоединенного к корпоративной сети и обменивающегося инфицированными данными с корпоративными серверами файл-приложений и баз данных;
- О распространение электронной почты, содержащей в приложениях файлы Excel и Word, инфицированные макровирусами.

Однако именно требование комплексного централизованного управления стало камнем преткновения для успешного создания эффективных комплексных систем антиви-

русной защиты корпоративных сетей в отечественных компаниях, что в конечном счете привело к столь широкому проникновению компьютерных вирусов в сети Internet/intranet.

Использование локальных антивирусных решений в корпоративной сети необходимо, но не достаточно для эффективной реализации антивирусной защиты предприятия. Сложившаяся сегодня ситуация требует незамедлительного вмешательства соответствующих должностных лиц и принятия решений, направленных на обеспечение и создание систем антивирусной защиты предприятия. По мнению многих специалистов, системы антивирусной защиты должны удовлетворять требованиям, приведенным в табл. 3.5.

Таблица 3.5. Основные требования к корпоративной системе антивирусной защиты

Функциональные возможности	Значение для корпоративного заказчика
Обнаружение вирусов	Принципиально важна, т. к. напрямую оправдывает финансовые затраты на приобретение и эксплуатацию антивирусного программного обеспечения
Обнаружение деструктивного кода типа «троянский конь», враждебные апплеты ActiveX, Java	Достаточно важна для корпоративного пользователя
Готовность быстрого реагирования на появление новых видов угроз	Актуальна способность производителя своевременно и быстро реагировать на появление новых угроз
Сопровождение и поддержка	Как правило, для пользователя важны ответы на следующие вопросы: «Какие составляющие входят в базовую конфигурацию?» «Что можно получить дополнительно» «Какие услуги входят в стоимость годовой технической поддержки?»
Исчерпывающий список защищаемых точек возможного проникновения вирусов	Вирусы и враждебные программы могут проникать из различных источников. Поэтому пользователи хотят быть уверенными в том, что не осталось ни одной незащищенной точки проникновения вирусов. Важно и периодическое централизованное обновление вирусных сигнатур
Управляемость	Возможность централизованного администрирования антивирусного программного обеспечения чрезвычайно актуальна. Так как нельзя полагаться на то, что конечные пользователи будут поддерживать работоспособность и обновление антивирусной защиты на своих рабочих станциях
Управление антивирусной защитой удаленных пользователей	Сейчас появилось большое количество пользователей, которые выполняют свою работу дома, подключаясь к ресурсам корпорации через компьютерную сеть и привнося новые точки проникновения вирусов. Поэтому администратору необходимо поддерживать их на том же уровне антивирусной защиты, что и тех, которые работают на локальных компьютерах
Централизованное уведомление	Пользователи понимают, что если они не смогут получить мгновенную единую картину всех уязвимых точек сети, они могут упустить из виду потенциальную, как правило, реальную вирусную атаку

Продолжение табл. 3.5

Производительность системы	Если антивирусная защита конфликтует с производительностью системы, доставкой почты или другими ключевыми аспектами современного процесса делового общения, у конечного пользователя появляется желание ее отключить
Удаленное администрирование (посредством браузера)	Если администратор сам является удаленным пользователем, интерфейс браузера дает ему возможность администрирования всего предприятия независимо от своего местонахождения
Автоматическое распространение и обновление	Сегодня администраторы могут быть ответственны за сотни рабочих станций и десятки различных сегментов сети предприятия, навестить которые самостоятельно невозможно. Поэтому понятно требование администратора, который хочет при помощи антивирусного программного обеспечения автоматизировать процесс автоматического распространения и обновления

Лучший способ борьбы с вирусной атакой — ее предотвращение. Для решения этой задачи необходимо:

- соответствующим образом сконфигурировать антивирусное программное обеспечение;
- использовать только лицензионное программное обеспечение;
- ограничить набор программ, которые пользователь способен установить в системе;
- устранить известные уязвимости в используемом программном обеспечении;
- контролировать использование накопителей гибких дисков и дисков CD-ROM;
- G разработать политику обработки электронной почты;
- разработать политику безопасности приложений, обрабатывающих документы с интерпретируемыми языками.

Чтобы соответствующим образом сконфигурировать антивирусное программное обеспечение, необходимо произвести следующие установки антивируса:

- сканирование в режиме реального времени, в фоновом или аналогичном режиме, должно быть разрешено;
- при старте системы нужно сканировать память, загрузочный сектор и системные файлы;
- своевременно обновлять вирусные базы данных;
- желательно сканировать файлы всех типов или, как минимум, COM-, EXE-файлы, а также файлы типа VBS, SHS, OCX;
- установить аудит всех действий антивирусных программ.

Поскольку программное обеспечение, полученное из неизвестного источника, может быть троянским или зараженным вирусом, то необходимо пользоваться только лицензионным программным обеспечением.

Ограничение набора программ, которые пользователь способен установить в системе, связано с тем, что эти программы могут быть заражены вирусами или служить причиной успеха других атак. Особо следует обратить внимание на различные сервисы Internet и, в первую очередь, на программы передачи сообщений, такие как IRC, ICQ, Microsoft Chat (они могут передавать файлы и служить источником заражения системы).

Для устранения известных «дыр» в используемом программном обеспечении в качестве источника информации об уязвимостях можно использовать базы данных, которые обычно публикуются в списках рассылки Internet, а также на специальных сайтах.

Вся информация, содержащаяся на гибких и компакт-дисках, должна быть проверена на наличие вирусов до того, как с ней будут работать пользователи компьютерной системы.

В связи с тем, что сообщения электронной почты — один из самых популярных и быстрых способов распространения вирусов, в каждой организации должна быть разработана политика обработки электронной почты. Для защиты от проникновения вирусов через сообщения электронной почты каждый пользователь системы должен:

- никогда не открывать сразу почтовое вложение в пришедшем ему сообщении, а сохранять его в определенном «карантинном» каталоге;
- никогда не открывать почтовых вложений, которые не были запрошены или о которых не было уведомления от отправителя (даже когда отправитель известен, сообщение может содержать вирус, если отправитель неизвестен, сообщение с вложением лучше всего удалить);
- перед открытием вложения обязательно проверить его с помощью антивирусного программного обеспечения;
- если после выполнения всех этих процедур остались сомнения, стоит связаться с отправителем и выяснить у него информацию о посланном вложении;
- устранить возможные уязвимости в клиентском почтовом программном обеспечении.

Если пользователь или организация используют приложения, обрабатывающие документы с интерпретируемыми языками (например, семейство продуктов Microsoft Office), то порядок работы с этими документами тоже должен быть отражен в политике безопасности.

Рассмотрим более подробно, как работают антивирусные программы и какие разновидности этих программ бывают.

Обычно анализ вирусов заключается в выделении в них сигнатур и последующем их поиске в потенциальных объектах вирусной атаки. Таким образом, еще несколько лет назад достаточно было поймать вирус, изучить его код (для профессионалов это, как правило, было делом нескольких минут) и выделить сигнатуру. Но вирусные технологии не стояли на месте. Разрабатывались новые вирусы, а вслед за ними и новые программные антивирусные продукты.

Антивирусных средств довольно много. А так как в каждом конкретном случае надо выбирать антивирусный комплект, исходя из общей концепции информационной безопасности организации и нужд конкретного пользователя, то ниже кратко описаны основные типы антивирусных средств.

Существуют следующие стандартные программы защиты (табл. 3.6):

- детекторы (scanner);
- фаги (полифаги) (scanner/cleaner, scanner/remover);
- ревизоры;
- сторожа;
- специальные вакцины;
- блокировщики.

Таблица 3.6. Стандартные антивирусные программы

Виды антивирусных программ	Назначение	Стандартные программы
Детекторы	Обнаружение вирусов	DrWeb AVP Adinf
Фаги (полифаги)	Обнаружение и уничтожение вирусов	Aidatest
Ревизоры	Контроль путей распространения вирусов	ADinf
Сторожа	Контроль подозрительных на вирус операций	VSAFE
Специальные вакцины	Обработка файлов и загрузочных секторов на устойчивость к вирусам	
Блокировщики	Ограничение распространения вирусов	—

В большинстве случаев вирус, заразивший компьютер, помогут обнаружить уже разработанные программы-детекторы. Они проверяют, имеется ли в файлах на указанном пользователем диске специфическая для данного вируса последовательность байт. При обнаружении вируса программа выводит на экран соответствующее сообщение. Назначение детектора — только обнаружить вирус. Бороться с ним предстоит либо другой антивирусной программе, либо системному программисту.

Среди детекторов можно выделить эвристические анализаторы кода — набор подпрограмм, анализирующих код исполняемых файлов, памяти или загрузочных секторов для обнаружения в нем разных типов компьютерных вирусов. Рассмотрим универсальную схему такого кодоанализатора. Действуя в соответствии с этой схемой, кодоанализатор способен максимально эффективно задействовать всю информацию, собранную для тестируемого объекта.

Эвристический подход состоит в попытке предложить, может быть, далекое от оптимального, но быстрое решение для чрезвычайно сложных (или даже неразрешимых) проблем на основе все более и более достоверных предположений.

Основная идея такого подхода состоит в том, что эвристика сначала рассматривает поведение программы, а затем сопоставляет его с характерным для злонамеренной атаки, наподобие поведения троянского коня. Установить модель поведения и принять решение относительно него можно с помощью нескольких механизмов. Для того чтобы выявить и определить все возможные действия программы, используют два подхода:

- сканирование;
- эмуляция.

Подход со сканированием предполагает поиск «поведенческих штампов», например, наиболее типичных низкоуровневых способов открытия файлов. Или процедура сканирования обычного исполняемого файла просматривает все места, где программа открывает другой файл, и определяет, какого рода файлы она открывает и что в них записывает.

Второй метод определения поведения — эмуляция. Такой подход несколько сложнее. Программа пропускается через эмулятор Windows или макроэмулятор Macintosh или Word с целью посмотреть, что она будет делать. Однако возникают вопросы, потому что в этом случае многое зависит от причуд вирусов. Например, если вирус запрограммирован на форматирование вашего жесткого диска 25 февраля в 10 час. утра, а при эмуляции этого вируса на симуляторе дата установлена на 24 февраля, то вирус пока не проявит свои намерения.

Вся хитрость быстрого распознавания состоит в сочетании двух подходов и получении наиболее подробного каталога поведенческих штампов за возможно более короткое время. Для проверки факта заражения файла вирусом специалисты могут использовать различные варианты искусственного интеллекта — экспертные системы и нейронные сети.

Недостаток эвристического подхода состоит как раз в его эвристичности. Всегда есть вероятность, что чрезвычайно подозрительный файл в действительности совершенно безобиден. Однако последний эвристический механизм Symantec под названием Bloodhound позволяет обнаружить до 80% неизвестных вирусов выполняемых файлов и до 90% неизвестных макровирусов.

Стоит также заметить, что программы-детекторы не слишком универсальны, поскольку способны обнаружить только известные вирусы. Некоторым таким программам можно сообщить специальную последовательность байт, характерную для какого-то вируса, и они смогут обнаружить инфицированные им файлы: например, это умеют NotronAntiVirus или AVP-сканер.

Программа Aidstest устарела и сейчас уже практически не используется. Наиболее широкое распространение получили программы DrWeb и AVP. Благодаря своим новейшим детекторам, они могут обнаружить любые вирусы: как самые старые, так и только что появившиеся. Еще нужно упомянуть детектор ADinf. Эта антивирусная программа обнаруживает все вирусы, не изменяющие длину файлов, невидимые вирусы, и многие другие. Таким образом, эти три программы обеспечивают мощнейшую защиту против вирусов. Все эти программы можно вписать в файл AUTOEXEC.BAT, тогда при загрузке компьютера проверка на заражение вирусом будет проводиться автоматически. Кстати, на Западе тоже предпочитают пользоваться такими российскими программами, как DrWeb и AVP.

Несколько лет назад детекторы практически уступили свои позиции программам, называемых полифагами, но сегодня они вновь возвращаются на компьютерный рынок.

Для тех, кто пользуется только лицензионным программным обеспечением, нет необходимости тратить время на лечение зараженных вирусом файлов. Проще восстановить зараженную программу с дистрибутива. Но в связи с тем, что даже во многих достаточно крупных организациях очень часто используют не лицензионную, а «пиратскую» продукцию (возможно, уже зараженную вирусом), то и чистые детекторы (сканеры) еще не скоро будут в состоянии конкурировать с фагами.

Фаги (полифаги) (scanner/cleaner, scaner/remover) — программы, способные не только обнаруживать, но и уничтожать вирусы, т. е. лечить «больные» программы (полифаг может уничтожить много вирусов). К полифагам относится и такая старая программа, как Aidstest, которая обнаруживает и обезвреживает около 2000 вирусов.

Основной принцип работы традиционного фага прост и секретом не является. Для каждого вируса путем анализа его кода, способов заражения файлов и т. д. выделяется некоторая характерная только для него последовательность байт. Эта последовательность называется сигнатурой данного вируса. Поиск вирусов в простейшем случае сводится к поиску их сигнатур (так работает любой детектор). Современные фаги используют другие методы поиска вирусов.

После обнаружения вируса в теле программы (или загрузочного сектора, который тоже, впрочем, содержит программу начальной загрузки) фаг обезвреживает его. Для этого разработчики антивирусных средств тщательно изучают работу каждого конкретного вируса: что он портит, как он портит, где он прячет то, что испортит (если прячет, конечно). В большинстве случаев фаг в состоянии благополучно удалить вирус и восстановить работоспособность испорченных программ. Но необходимо хорошо понимать, что это возможно далеко не всегда.

Программы, называемые ревизорами, контролируют возможные пути распространения инфекции. Изобретательность авторов вредоносного программного обеспечения ограничена некоторыми рамками, исходя из того, возможно в принципе. Эти рамки хорошо известны и поэтому вирусы все же не всесильны. Если взять под контроль все мыслимые направления вирусной атаки на компьютер, то можно находиться практически в полной безопасности. Из программ-ревизоров, которые можно приобрести в России, следует обратить внимание на уже упомянутую выше программу ADinf.

Сторожами называют небольшие резидентные программы, находящиеся постоянно в памяти компьютера и контролирующие операции, которые они считают подозрительными. В качестве примера программы-сторожа можно привести программный продукт VSAFE, входивший в поставку некоторых версий MS DOS.

Поскольку и вирусы, и обычные программы выполняют одни и те же операции, то невозможно даже выделить класс исключительно «вирусных» операций. Вследствие этого сторож либо вынужден ничего не контролировать и пассивно наблюдать за происходящим, либо «звенеть» при каждой подозрительной операции. Поэтому целесообразно использовать программы-сторожа на самом минимальном уровне контроля (например, отслеживания изменений загрузочных секторов). Такими сторожевыми функциями обладают некоторые современные BIOS, хотя и с этим все не так просто. Эта функция BIOS может конфликтовать с некоторыми операционными системами, а иногда может вообще не работать.

Специальные вакцины предназначены для обработки файлов и загрузочных секторов. Вакцины бывают пассивными и активными. Активная вакцина, «заражая» файл, подобно вирусу, предохраняет его от любого изменения и в ряде случаев способна не только обнаружить сам факт заражения, но и вылечить файл. Пассивные вакцины применяют только для предотвращения заражения файлов некоторыми вирусами, использующими простые признаки их зараженности — «странные» время или дата создания, определенные символьные строки и т. д.

В настоящее время вакцинирование широко не применяется. Бездумное вакцинирование всего и вся способно вызвать целые эпидемии несуществующих вирусных болезней. Так, в течение нескольких лет на территории бывшего СССР свирепствовала страшная эпидемия ужасного вируса TIME. Жертвой этого вируса стали сотни абсолютно здоровых программ, обработанных антивирусной программой ANTI-KOT.

Приведем пример из практики. В настоящее время имеется довольно много вирусов, предотвращающих повторное заражение файлов некоторой «черной меткой», которой они метят инфицированную программу. Существуют, к примеру, вирусы, выставляющие в поле секунд времени создания файла значение 62. Уже довольно

давно появился вирус, который ко всем зараженным файлам дописывал пять байт — MsDos. Нормальных файлов, содержащих в конце такую символьную строку, не бывает, поэтому вирус и использовал этот признак как индикатор заражения файла. Вакцинирование файлов против такого вируса совсем не сложно. Достаточно дописать в конец выше упомянутую символьную строку — и заражение таким вирусом вам не страшно. Страшно другое — некоторые антивирусные программы, встретив в конце файла злополучную строчку, начинают немедленно лечить его. Шансов на то, что после такого «лечения» «инвалид» будет нормально работать, практически никаких.

Еще одной разновидностью антивирусных программ являются блокировщики вируса. Они позволяют ограничить распространение эпидемии, пока вирус не будет уничтожен. Практически все резидентные вирусы определяют факт своего присутствия в памяти машины, вызывая какое-либо программное прерывание с «хитрыми» параметрами. Если написать простую резидентную программу, которая будет имитировать наличие вируса в памяти компьютера, правильно «отзываясь» на определенный пароль, то вирус, скорее всего, сочтет эту машину уже зараженной.

Даже если некоторые файлы на компьютере содержат в себе код вируса, при использовании блокировщика заражения всех остальных файлов не произойдет. Для нормальной работы такой программы необходимо запустить блокировщик раньше всех остальных программ, например, в файле CONFIG.SYS. Но если вирус успел заразить COMMAND.COM или стартует из загрузочного сектора, то антивирус-блокировщик не поможет.

Очень важно применять альтернативные антивирусные решения. Сами по себе антивирусные сканеры и настройки защиты в различных приложениях не обеспечивают адекватной защиты от вредоносных программ. Антивирусные сканеры необходимо постоянно обновлять, хотя быстро распространяющиеся вирусы могут опередить эти модернизации.

Единственный способ избежать воздействия вредоносного программного обеспечения — блокировать подозрительные файлы на межсетевом экране или на шлюзе электронной почты. Многие организации сейчас блокируют все входящие присоединенные файлы, имеющие следующие, потенциально опасные, расширения: EXE, CORN, SCR, HTA, HTO, ASF, CHM, SHS, PIF. Другие устанавливают еще более жесткие фильтры, блокируя файлы с расширениями ADE, ADP, BAS, BAT, CMD, CNT, CPL, CRT, CSS, HIP, INF, INS, ISP, JS, JSE, INK, MDB, MDE, MSC, MSI, MSP, MST, PCD, REG, SET, SHB, URI, VB, VBE, VBS, WSC, WSF, WSH.

Один из ключевых вопросов, который будет стоять перед индустрией детектирующих систем в течение ближайших лет, заключается в том, продолжат ли заказчики покупать эти системы как самостоятельные продукты или уже скоро они станут приобретать их в комплекте с сетевым оборудованием — маршрутизаторами, коммутаторами или устройствами для локальных сетей. Ответ на него пока не найден, однако не приходится сомневаться, что системы выявления сетевых атак, используемые сегодня преимущественно такими крупными организациями, как банки и федеральные учреждения, со временем найдут дорогу к более широким слоям корпоративных пользователей.

Практические методы и средства для защиты сети от вредоносных программ

Программные средства, уведомляющие администратора об атаке на сервер или сеть либо только о попытке такой атаки, появились совсем недавно. Первые продукты этого типа были апробированы военным ведомством США в середине 90-х годов. Тем не менее за прошедшие несколько лет растущая армия поставщиков программного обеспечения успела выпустить несколько пакетов программ, нацеленных на выявление хакерских атак. Одни производители предлагают серверные продукты, обеспечивающие защиту операционных систем, Web-серверов и баз данных. Другие рассматривают проблему защиты с общесетевых позиций, и их разработки позволяют сканировать весь сетевой трафик для выявления пакетов сомнительного происхождения.

Что касается экономической стороны дела, то рынок детектирующих систем обоих типов бурно развивается. По данным компании IDC, в 1997 году его оборот составлял 20 млн долларов, а уже в 2000 году достиг 100 млн долларов. Оценки дальнейшего развития весьма оптимистичны: аналитики IDC полагают, что мировые продажи программ обнаружения сетевых атак в 2005 году перевалят за 500 млн долларов.

В такой сфере, как обнаружение сетевых атак, процесс совершенствования бесконечен. Хакеры не устают изобретать все новые схемы проникновения в компьютерные системы. Стоящие по другую сторону баррикад разработчики детектирующих приложений отслеживают появляющиеся новинки и спешат предложить свои контрмеры. Вот почему выпускаемые продукты требуют постоянной модернизации и пользователям настоятельно рекомендуется устанавливать обновленные сигнатуры, позволяющие идентифицировать новые виды сетевых атак.

Старое антивирусное программное обеспечение подобно лекарству с истекшим сроком годности — толку от него мало. Если не обновлять файлы сигнатур, то рано или поздно можно оказаться беззащитными против новых вирусов. Большинство фирм, производящих антивирусы, выпускают новые файлы сигнатур по крайней мере два раза в месяц и чаще, если появляется серьезный вирус. Для получения новых сигнатур удобно пользоваться функцией автоматического обновления через Web, имеющейся в антивирусном пакете.

Сопровождение через Internet программы PC-cillin, например, обладает уникальной особенностью. Вы можете не только запросить консультацию по электронной почте, но и в любое время суток поболтать в реальном времени со специалистом службы сопровождения Trend. (Разумеется, от этой замечательной услуги не особенно много проку, если компьютер заблокирован и войти в Internet невозможно, однако она бесплатна.)

Такие антивирусные продукты, как Norton AntiVirus 2000 и McAfee VirusScan, поддерживают самые крупные исследовательские группы отрасли: соответственно Symantec AntiVirus Research Center и AntiVirus Emergency Response Team. Поэтому Norton и McAfee исключительно быстро реагируют на угрозу нового вируса.

Чтобы снизить число дорогостоящих телефонных консультаций, антивирусные компании стараются усилить поддержку

через Internet. Но иногда все-таки бывает нужно задать вопрос живому человеку. Если вы купили продукт, то, скорее всего, получите сопровождение по телефону и через Internet бесплатно, а вот в случае бесплатных пакетов поддержка будет стоить денег.

Все основные фирмы-поставщики антивирусного обеспечения регулярно и притом часто обновляют файлы сигнатур вирусов, а при появлении особо зловредного вируса делают дополнительный экстренный выпуск. Еще совсем недавно считалось, что сигнатуры нужно обновлять ежемесячно, но в нашу эпоху новых отвратительных вирусов, возможно, будет разумным проверять их каждую неделю вручную или с помощью автоматического обновления антивирусной программы. В утилитах McAfee, Symantec и Trend Micro для обновления достаточно один раз щелкнуть кнопкой мыши.

Распространение противоядия в рамках корпоративной среды возвращает нас обратно к вопросу времени реакции со стороны поставщика антивирусных средств. Конечно, доставка сигнатур новых вирусов на настольные системы чрезвычайно важна, но для того чтобы их распространять, эти сигнатуры надо сначала получить. В идеале их хотелось бы иметь до того, как ваш компьютер будет атакован.

Обычно поставщик антивирусных средств дает ответ в течение не более двух суток после предоставления ему подозрительного файла (срок в 48 час. стал, по сути, стандартной верхней границей). Однако в наши дни 48 час. — это слишком долго, за это время могут быть инфицированы тысячи рабочих станций. Можно это делать быстрее, используя автоматизацию, которая будет играть все более важную роль в разрабатываемых централизованных корпоративных системах, куда выявленные с помощью эвристических средств образцы можно направлять на карантин и откуда их передают поставщику антивирусных средств. В этом случае анализ образцов поставщиком может быть автоматизирован. Под этим подразумевается автоматическое тиражирование образцов, определение наличия инфекции, автоматическое создание лекарства для этой инфекции, автоматическая проверка лекарства и передача его обратно корпоративному клиенту и любым другим клиентам этой сети. Результат — вместо обещаемых большинством компаний 48 час. вся процедура продлится около получаса, и даже быстрее.

Компания Symantec, например, уже сегодня располагает подобной системой для макровирусов, т. е. вирусов Word for Windows и Excel. Ей требуется два часа, чтобы предоставить вам набор определений для противодействия новому вирусу (если он никогда ранее не встречался), — и все это исключительно посредством компьютера.

Определенный набор средств антивирусной защиты присутствует во всех утилитах основных фирм-производителей программного обеспечения. Таковы постоянная защита от вирусов (антивирусный монитор), проверка системы по расписанию и обновление сигнатур через Internet, а также создание аварийной загрузочной дискеты, позволяющей запустить компьютер даже тогда, когда у него заражен вирусом загрузочный сектор (естественно, дискету надо создать до того, как вирус попал в компьютер). Помимо этих стандартных средств, некоторые пакеты содержат «архитектурные излишества»: например, специальную добавочную защиту от почтовых вирусов (тревога по поводу которых нарастает), а также зловредных модулей ActiveX и Java-апплетов (которые до сих пор редкость). А такие программы, как Panda Antivirus Platinum и PC-cillin, даже позволяют родителям заблокировать доступ детей к нежелательным Web-страницам. Характеристики категорий антивирусного программного обеспечения представлены в табл. 3.7.

Таблица 3.7. Характеристики категорий антивирусного программного обеспечения

Категория	Название антивирусного программного обеспечения	Характеристика антивирусов
I	Command Antivirus	Деловой подход, простота, доступность, реагируют на угрозу нового вируса
	F-Secure	
II	Inoculate IT	Высокая скорость распознавания вирусов, пропуск вирусов
	Norman Virus Control	
III	Norton Antivirus	Лучший антивирус по всем показателям
	McAfee Virus Scan	Большая информативность
	Panda Antivirus Platinum	Блокируют доступ компьютеров к нежелательным Web-страницам. Возможность консультации по электронной почте
	PC-cillin	

Поскольку у новых вирусов имеются новые сигнатуры, файлы сигнатур необходимо поддерживать в актуальном состоянии. При выходе новой версии антивируса формат файла сигнатур обычно меняется, и обновленные сигнатуры оказываются несовместимы с предыдущими версиями программы. Именно поэтому антивирусное программное обеспечение уже довольно давно продается по той же схеме, что бритвы и лезвия: однажды купив основную утилиту (бритву), вы затем вынуждены постоянно покупать обновленные файлы сигнатур (лезвия).

Так, компании McAfee и Symantec предоставляют право неограниченного обновления сигнатур в течение года с момента приобретения утилиты, но за каждый следующий год нужно в обоих случаях заплатить 4 доллара. Такую сумму вряд ли можно считать серьезным ударом по карману (в отличие от подписки на обновленные файлы сигнатур F-Secure, которая стоит 63 доллара); кроме того, через год вы с большой вероятностью захотите обновить саму программу. Их основные конкуренты — Command AntiVirus, Inoculate IT, Panda Antivirus Platinum и PC-cillin — предлагают бесплатное обновление сигнатур в течение всей жизни продукта.

В настоящее время способы предоставления антивирусной защиты существенно меняются. Компания McAfee.com (существующая отдельно от McAfee Software) уже предлагает проверку на вирусы через Internet в своей «электронной больнице» McAfee Clinic (наряду с еще несколькими видами диагностики). Услуга предоставляется по подписке и стоит 50 долларов в год, но часто появляются специальные предложения, а за первые две недели плата не берется — это испытательный период. Проверку удаленных компьютеров на вирусы производит модуль ActiveX, который берет сигнатуры с Web-сервера производителя программы.

К сожалению, сегодня производители не располагают какими бы то ни было сверхновыми технологиями для упрощения процедуры постоянной модернизации приобретенного заказчиками программного обеспечения. Более того, даже самостоятельная загрузка пользователями обновлений для базы данных с сервера производителя, ставшая общим местом в индустрии антивирусного программного обеспечения, для поставщиков средств обнаружения сетевых атак пока еще в диковинку.

В качестве потенциального выхода из создавшегося положения эксперты по системам сетевой безопасности рассматривают применение технологий искусственного

интеллекта. Они позволили бы распознавать угрозы отдельным компьютерам или сети в целом без использования файлов сигнатур, требующих постоянного обновления. Отдельные продукты предоставляют пользователям возможность добавлять в систему собственные сигнатуры сетевых атак (например, для защиты специфических приложений). Такая гибкость достигается путем включения в комплект поставки дополнительных инструментальных средств.

Существенным недостатком многих систем обнаружения атак является их неспособность выдавать предупреждающие сообщения на консоли основных платформ сетевого администрирования. Диагностическая информация и отчеты о событиях, как правило, объединяются только на их собственных управляющих станциях. Это затрудняет принятие ответных мер против хакера.

Системы выявления сетевых атак, предлагаемые фирмами Network Associates и ISS, способны взаимодействовать с рядом брандмауэров и платформ сетевого администрирования, однако в настоящее время эти компании заняты реализацией технологии автоматического реагирования на попытки несанкционированного доступа, что предполагает более активное участие представителей всей сетевой индустрии. Основная идея такой технологии состоит в установке на хостах и отдельных сетевых устройствах «сканеров» сетевых атак, которые при обнаружении серьезной угрозы информационной безопасности могли бы активизировать средства защиты без вмешательства администратора.

Сети становятся все более уязвимыми к инфицированным сообщениям электронной почты. Этому способствует интерактивный характер приложений, незакрытые бреши в системах защиты и постоянное совершенствование вирусных программ. Вирусы, подобные LoveLetter и Prolin, способны самотиражироваться по электронной почте, используя недостатки таких программ, как Microsoft Outlook и Outlook Express. В силу активного характера каждого из этих вирусов за считанные часы могут быть разосланы тысячи инфицированных сообщений, в результате чего вирусы окажутся в системе других клиентов. Вирус Melissa, появившийся в марте 1999 года, стал первым широко распространенным размножающимся по почте вирусом и вызвал многочисленные сбои на корпоративных серверах электронной почты, буквально засыпав их огромным количеством сообщений. Созданный тоже не так давно вирус LoveLetter точно так же поразил серверы электронной почты. По некоторым оценкам, ущерб от него в различных организациях по всему миру составил несколько миллиардов долларов.

Помимо переполнения системы электронной почты, вирус может повредить файлы, переслать конфиденциальную информацию путем рассылки документов, инициировать атаку на отказ от обслуживания (Denial of Service, DoS), изменить и удалить конфигурационные настройки, хранящиеся в памяти CMOS и во Flash BIOS системных плат некоторых типов.

Как правило, для доставки своего «смертоносного груза» вирусы используют код HTML в теле сообщения электронной почты. Вирус KakWorm, например, скрывается в подписи, передаваемой вместе с сообщениями электронной почты MS Outlook Express 5. Он написан на JavaScript и распространяется через английскую и французскую версии Windows 95/98. Этот червь заражает систему в тот момент, когда пользователь открывает или просто просматривает инфицированное сообщение электрон-

ной почты. Поскольку многие так и не установили необходимую заплатку для Outlook, этот вирус по-прежнему широко распространен, хотя впервые он был обнаружен еще в октябре 1999 года.

На программы электронной почты MS Outlook и Outlook Express рассчитано немало вирусов, в том числе Bubble-Boy, Stages, Lucky, Melissa, NewLove и LoveLetter. Хотя некоторые из наиболее распространенных вирусов и «червей» появляются на настольной системе пользователя как код HTML в теле сообщения, многие, тем не менее, рассылаются в виде прикрепленных файлов, зачастую с «замаскированными» расширениями. Чаще всего они представляют собой файлы в формате DOC, внутри которых находятся вредоносные макросы. Хотя количество макровирусов продолжает быстро расти, подавляющее число инцидентов связано с вирусами, рассылающими себя по электронной почте.

Хотя основную угрозу представляет традиционный вредоносный код, проблемы может вызвать и код иного типа. Например, внешний вид многих коммерческих Web-сайтов формируется с помощью апплетов JavaScript и элементов управления ActiveX. Чтобы эта схема работала, пользователь должен загрузить данный мобильный код на настольную систему, где тот получает доступ к жесткому диску. Код такого типа может читать, удалять и изменять файлы, а кроме того, способен обращаться к файлам на компьютерах, подключенных к данному через локальную сеть.

Поскольку апплеты Java относят к не вызывающему доверия коду, они работают внутри виртуальной машины в так называемой «песочнице». Теоретически это призвано ограничить выполняемые ими операции и уберечь от несанкционированных действий компьютер пользователя. Зачастую ActiveX воспринимается как более серьезная угроза, потому что, по существу, он представляет собой компактную версию OLE, позволяющую напрямую обращаться к оригинальным вызовам Windows и связывать их с любой системной функцией.

Более того, поскольку хакер может присоединить апплет Java к электронной почте, браузер способен автоматически активировать этот апплет. Узнать, на какие разрушительные действия способно вредоносное программное обеспечение на основе JavaScript и ActiveX, можно на многих сайтах.

Основную проблему, сдерживающую широкое распространение продуктов рассматриваемого класса, представляют заоблачные цены, которые оказываются не по зубам небольшим компаниям — самой легкой добыче злоумышленников. Скажем, типичная стоимость серверного агента в таких системах составляет 4000 долларов. В результате большинство организаций вынуждены устанавливать детектирующее программное обеспечение только на наиболее уязвимых сетевых узлах, например, на брандмауэрах или на серверах с конфиденциальной информацией делового характера.

Однако, все не так уж плохо, как кажется на первый взгляд. Корпоративные заказчики, например, могут теперь оперативно решить проблемы информационной безопасности благодаря растущему предложению коммерческих услуг в этой области со стороны независимых фирм.

Это связано с тем, что сегодня налицо дефицит специалистов высокой квалификации в области сетевой безопасности, да к тому же обладающих практическим опытом обнаружения хакерской активности. Поэтому организации предпочитают делегировать решение возникающих задач немногочисленным специализированным компаниям.

Можно также обратиться к компаниям, оказывающим специализированные услуги по организации безопасности информационных систем. Они обычно предлагают целый пакет услуг, включающий в качестве базовых компонентов межсетевые экраны и системы выявления вторжений (Intrusion Detection System, IDS). В пакет услуг может входить и оценка слабых мест в системе защиты, и проверка возможности проникновения в систему, и централизованная защита и др. Это, конечно, недешево, но такие трудоемкие задачи, как мониторинг работы межсетевого экрана и журналов системы выявления вторжений (IDS), не слишком дороги, зато сэкономят время для не менее важных дел.

Для улучшения качества антивирусной защиты необходимо обучать пользователей. Правила, действующие вчера, сегодня уже не работают. Пользователей необходимо информировать о возможном риске, они должны быть особенно внимательны при просмотре электронной почты и работе с ней. Кроме того, важно, чтобы они предвидели неприятные последствия об изменении настроек защиты или установки программного обеспечения, не являющегося корпоративным стандартом.

Компьютерная безопасность требует, чтобы ей каждый день уделялось время и внимание. Устанавливая очередную «заплату», внимательно наблюдая за появлением новых уязвимых мест в системе, повышая свою квалификацию и изучая опыт более осведомленных в этой области людей, вы можете поддерживать свою сеть в стабильном состоянии. Квалифицированный администратор сетевой безопасности — вот отличная защита от незаконных вторжений в информационную систему. Поэтому лучшей инвестицией станет обучение сотрудников, ответственных за безопасность. Но ничто не сравнится с практическим обучением. А для этого потребуется собственная лаборатория, где администраторы могли бы экспериментировать без опасения помешать работе основной сети.

Но это в общем. А что делать пользователю, если заражение уже произошло? Прежде всего, не надо паниковать. Первый шаг при обнаружении атаки на систему — это ее идентификация. Для успешной идентификации атаки необходимо наличие загрузочного диска, создаваемого при установке системы, и осуществление загрузки системы с его помощью.

Если атака идентифицируется антивирусом, проблема решается фактически моментально. Но, если вы имеете дело с неизвестным вирусом, во многих случаях критичным является время, за которое была идентифицирована атака. Поэтому решающее значение имеет способность пользователя быстро обнаружить вирусную атаку (признаками могут служить массовая рассылка почты, уничтожение файлов и т. д.). Сложность идентификации часто зависит от сложности самой атаки. На данном этапе желательно установить, как минимум, следующие признаки:

- сам факт атаки;
- тип атаки (сетевая или локальная);
- источник происхождения.

Вне зависимости от типа операционной системы необходимо обращать внимание на следующую активность в системе:

- О целостность программного обеспечения, используемого для обнаружения нарушителя;
- целостность критичных для безопасности системы программ и данных;
- операции в системе и сетевой трафик.

Если вы смогли определить факт вирусного заражения неизвестным вирусом (или у вас есть такие небезосновательные подозрения), то желательно обратиться к производителю используемого антивирусного программного обеспечения. Кроме того, необходимо проанализировать последствия вирусной атаки. Если в вашей системе обрабатывались какие-то ценные данные, то настоятельно рекомендуется иметь их резервную копию. Для этого должны быть разработаны правила резервного копирования. К сожалению, если резервная копия отсутствует, данные могут быть утеряны навсегда (это уже зависит не от вас, а от злоумышленника, написавшего вирус).

В любом случае необходимо помнить: наличие адекватных средств защиты и дисциплины их применения позволяет если не избежать вирусной атаки, то, по крайней мере, минимизировать ее последствия. Для этого всегда проверяйте файлы, попадающие на ваш компьютер. Нужно помнить, что любой из них может быть заражен вирусом. Никогда не позволяйте посторонним работать на вашем компьютере — именно они чаще всего приносят вирусы. Особое внимание следует уделять играм: ведь часто вирусы распространяются именно так. Новые игры и программы всегда нужно проверять на наличие вирусов. Кажется очевидным, что лучше чуть-чуть потесниться и найти 8-12 кбайт свободного места в оперативной памяти, скажем в UMB, где можно разместить «недремлющее око» резидентного монитора, контролирующее все вирусоподобные проявления и предотвращающее малейшие попытки вирусного заражения. А сканировать лучше прямо на сервере, так как в сетевых антивирусных системах это обычная опция.

В большинстве организаций антивирусное программное обеспечение установлено, по крайней мере, на настольных компьютерах. Весьма разумным вложением средств было бы также добавление антивирусного программного обеспечения на шлюзы электронной почты и межсетевые экраны. Согласно данным опроса, проведенного в крупных организациях компанией Tru-Secure, большинство вирусов и другой вредоносный код попадают в систему через электронную почту. Выявление как можно большего числа потенциальных проблем на основной точке входа в систему значительно сокращает внутренние работы.

К сожалению, большая часть антивирусного программного обеспечения плохо сконфигурирована и анализирует лишь часть потенциально инфицированных объектов. В электронной почте и на настольной системе имеет смысл использовать сканер, настроенный так, чтобы он проверял все файлы. Учитывая, что содержать инфицированные объекты могут более 200 типов файлов, сканировать нужно не только файлы, расширение которых совпадает с одним из предлагаемого вместе с продуктом списка.

Кроме того, следует иметь в виду, что заданные по умолчанию в большинстве приложений настройки защиты неадекватны реальной среде. Поскольку исследователи обнаруживают все новые уязвимые места в продуктах, необходимо постоянно следить за выпуском новых «заплаток». Это можно сделать, подписавшись на бюллетень новостей по вопросам защиты компании Microsoft и других компаний, отслеживающих ошибки в программном обеспечении, например, на списки рассылки Security-Focus.

Применяемые средства защиты должны быть как можно более разнообразными, в частности, антивирусные сканеры от различных производителей на каждом рубеже системы защиты:

- межсетевых экранах;
- почтовых серверах;
- файловых серверах;
- настольных системах.

Эти многочисленные фильтры теоретически позволяют отсечь больше вирусов, поскольку часто разные продукты способны выявлять различные виды вредоносного программного обеспечения. Несмотря на рост затрат в случае применения различных сканеров (как правило, на разных уровнях системы защиты), преимущества перевешивают недостатки.

Многие преступления в сфере информационных технологий стали возможны благодаря тому, что хакеры находят бреши в программном обеспечении, которые позволяют легко обойти сетевую защиту Это происходит почти с каждой известной программой. В девяти случаях из десяти они используют в своих интересах старые, давно известные недоработки в программах, для которых уже существуют «заплаты», которые не успели или не побеспокоились применить.

Теоретически установка «заплаты» не так уж сложна, хотя на практике не все так просто даже для опытных администраторов, которые стараются быть в курсе самых последних разработок. Самое главное — не нужно опаздывать с установкой «заплат» в своей системе. При этом одна из трудностей заключается в том, что в информационных системах устанавливается все больше и больше новых программных продуктов. Количество же брешей, выявляемых еженедельно, увеличилось более чем в два раза за период с 1999 года по 2000 год. Хакеры могут использовать эти недоделки, чтобы проникнуть в компьютерные сети и вывести их из строя. В результате поставщики программного обеспечения вынуждены регулярно создавать «заплаты» на эти уязвимые места.

В руках сетевого администратора анализатор протоколов — весьма полезный инструмент, помогающий находить и устранять неисправности, избавляться от узких мест, снижающих пропускную способность сети, и обнаруживать проникновение в нее компьютерных взломщиков. Для тех, кто желает дать отпор компьютерным взломщикам, использующим анализаторы протоколов для организации атак на компьютерные системы, подключенные к сети, можно посоветовать следующее:

- обзаведитесь сетевым адаптером, который принципиально не может функционировать в беспорядочном режиме;
- приобретите современный сетевой интеллектуальный коммутатор;
- не допускайте несанкционированной установки анализаторов протоколов на компьютеры сети;
- шифруйте весь трафик сети.

Сетевые адаптеры, которые принципиально не могут функционировать в беспорядочном режиме, на самом деле существуют. Одни адаптеры не поддерживают беспорядочный режим на аппаратном уровне (их меньшинство), а остальные просто снабжаются драйвером, не допускающим работу в беспорядочном режиме, хотя этот режим и реализован в них аппаратно. Чтобы отыскать адаптер, не поддерживающий беспорядочный режим, достаточно связаться со службой технической поддержки любой компании, торгующей анализаторами протоколов, и выяснить, с какими адаптерами их программные пакеты не работают.

Учитывая, что спецификация PC99, подготовленная по инициативе корпораций Microsoft и Intel, требует безусловного наличия в сетевой карте беспорядочного режима, необходимо приобрести современный сетевой интеллектуальный коммутатор, который буферизует каждое отправляемое по сети сообщение в памяти и отправляет его по мере возможности точно по адресу. В результате отпадает надобность в «прослушивании» сетевым адаптером всего трафика для того, чтобы выбирать из него сообщения, адресатом которых является данный компьютер.

Чтобы не допустить несанкционированной установки анализаторов протоколов на компьютеры сети, следует применять средства из арсенала, который повсеместно используется для борьбы с программными закладками и, в частности, с троянскими программами.

Для шифрования всего трафика сети имеется широкий спектр программных пакетов, которые позволяют делать это достаточно эффективно и надежно. Возможность шифрования почтовых паролей предоставляется протоколом APOP (Authentication POP) — надстройкой над почтовым протоколом POP (Post Office Protocol). При работе с протоколом APOP по сети каждый раз передается новая зашифрованная комбинация, которая не позволяет злоумышленнику извлечь какую-либо пользу из информации, перехваченной с помощью анализатора протоколов. Проблема только в том, что не все почтовые серверы и клиенты поддерживают протокол APOP.

Другой продукт под названием Secure Shell (SSL) был изначально разработан финской компанией SSH Communications Security и в настоящее время имеет множество реализаций, доступных бесплатно через Internet. Программный продукт SSL представляет собой защищенный протокол для осуществления безопасной передачи сообщений по компьютерной сети с помощью шифрования.

Особую известность среди компьютерных пользователей приобрела серия программных пакетов, предназначенных для защиты передаваемых по сети данных путем шифрования и объединенных присутствием в их названии аббревиатуры PGP (Pretty Good Privacy).

Кроме программных, существуют и аппаратные средства защиты. Имеются специальные дополнительные устройства, обеспечивающие достаточно надежную защиту. В отличие от всех рассмотренных выше антивирусных средств, аппаратный комплекс Sheriff, например, способен предотвратить нападение вируса. К сожалению, всегда существуют области жесткого диска, не защищенные платой Sheriff, а такие области есть практически всегда. То есть если защитить винчестер целиком, то как же работать?

Необходимо помнить, что антивирусные средства должны применяться комплексно и только такая комплексная защита с использованием надежного ревизора (ADinf), фагов DrWeb и Aidstest, а при необходимости и платы Sheriff, способна обеспечить максимальную безопасность.

Помимо программного обеспечения для сканирования на наличие вирусов, есть еще, например, блокираторы действий, программы контроля доступа и модули проверки целостности. Эти программы препятствуют совершению злонамеренных действий или модификации существующих файлов, а не сканируют файлы в поиске известного вредоносного программного обеспечения. Такой подход обеспечивает

дополнительную защиту от атак, осуществляемых с помощью ActiveX, Java и другого разрушительного невирусного кода.

Подобные функции выполняют продукты таких производителей, как Aladdin, Computer Associates, Pelican Security, Sandbox Security, Stiller Research и Trend Micro. Они выявляют вредоносный код Java и ActiveX либо путем использования списков известных блоков кода, либо посредством выявления вредоносных действий.

Методы защиты от программных закладок

Признаки, выявляемые с помощью средств тестирования и диагностики, характерны как для компьютерных вирусов, так и для программных закладок. Например, загрузочные закладки успешно обнаруживаются антивирусными программами, которые сигнализируют о наличии подозрительного кода в загрузочном секторе диска. С инициированием статической ошибки на дисках хорошо справляется Disk Doctor, входящий в распространенный комплект утилит Norton Utilities. А средства проверки целостности данных на диске типа Adinf позволяют успешно выявлять изменения, вносимые в файлы программными закладками. Кроме того, эффективен поиск фрагментов кода программных закладок по характерным для них последовательностям нулей и единиц (сигнатурам), а также разрешение выполнения только программ с известными сигнатурами.

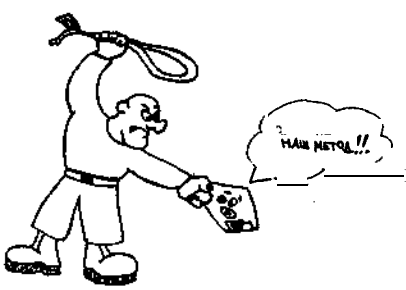
Выявление внедренного кода программной закладки заключается в обнаружении признаков его присутствия в компьютерной системе. Эти признаки можно разделить на следующие два класса:

- качественно-визуальные;
- обнаруживаемые средствами тестирования и диагностики.

К качественно-визуальным признакам относятся ощущения и наблюдения пользователя компьютерной системы, который отмечает определенные отклонения в ее работе (изменяются состав и длины файлов, старые файлы куда-то пропадают, а вместо них появляются новые, программы начинают работать медленнее или заканчивают работу слишком быстро, или вообще перестают запускаться).

Несмотря на то что суждение о наличии признаков этого класса кажется слишком субъективным, тем не менее, они часто свидетельствуют о наличии неполадок в компьютерной системе и, в частности, о необходимости проведения дополнительных проверок присутствия программных закладок средствами тестирования и диагностики.

Например, пользователи пакета шифрования и цифровой подписи «Криптоцентр» с некоторых пор стали замечать, что цифровая подпись под электронными документами ставится слишком быстро. Исследование, проведенное специалистами ФАПСИ, показало присутствие программной закладки, работа которой основывалась на навязывании длины файла. В другом случае тревогу забили пользователи пакета шифрования и цифровой подписи «Криптон», которые с удивлением отметили, что скорость шифрования по криптографическому алгоритму ГОСТ 28147-89 вдруг возросла более, чем в 30 раз. А в



третьем случае программная закладка обнаружила свое присутствие в программе клавиатурного ввода тем, что пораженная ею программа перестала нормально работать.

Задача защиты от программных закладок может рассматриваться в трех принципиально различных вариантах:

- ❑ не допустить внедрения программной закладки в компьютерную систему;
- ❑ выявить внедренную программную закладку;
- ❑ удалить внедренную программную закладку.

При рассмотрении этих вариантов защита от программных закладок сходна с защитой компьютерных систем от вирусов. Как и в случае борьбы с вирусами, задача решается с помощью средств контроля за целостностью запускаемых системных и прикладных программ, а также за целостностью информации, хранимой в компьютерной системе и за событиями, критическими для функционирования системы. Однако данные средства действенны только тогда, когда сами они не подвержены влиянию программных закладок, которые могут:

- ❑ навязывать конечные результаты контрольных проверок;
- ❑ влиять на процесс считывания информации и запуск программ, за которыми осуществляется контроль;
- Q изменять алгоритмы функционирования средств контроля.

При этом чрезвычайно важно, чтобы включение средств контроля выполнялось до начала воздействия программной закладки либо когда контроль осуществлялся только с использованием программ управления, находящихся в ПЗУ компьютерной системы.

Интересный метод борьбы с внедрением программных закладок может быть использован в информационной банковской системе, в которой циркулируют исключительно файлы-документы. Чтобы не допустить проникновения программной закладки через каналы связи, в этой системе не допускается прием никакого исполняемого кода. Для распознавания событий типа «ПОЛУЧЕН ИСПОЛНЯЕМЫЙ КОД» и «ПОЛУЧЕН ФАЙЛ-ДОКУМЕНТ» применяют контроль за наличием в файле запрещенных символов: файл считается содержащим исполняемый код, если в нем присутствуют символы, которые никогда не встречаются в файлах-документах.

Конкретный способ удаления внедренной программной закладки зависит от метода ее внедрения в компьютерную систему. Если это программно-аппаратная закладка, то следует перепрограммировать ПЗУ компьютера. Если это загрузочная, драйверная, прикладная, замаскированная закладка или закладка-имитатор, то можно заменить их на соответствующую загрузочную запись, драйвер, утилиту, прикладную или служебную программу, полученную от источника, заслуживающего доверия. Наконец, если это исполняемый программный модуль, то можно попытаться добыть его исходный текст, убрать из него имеющиеся закладки или подозрительные фрагменты, а затем заново откомпиллировать.

Универсальным средством защиты от внедрения программных закладок является создание изолированного компьютера (рис. 3.37). Компьютер называется изолированным, если выполнены следующие условия:

- Q в нем установлена система BIOS, не содержащая программных закладок;
- Q операционная система проверена на наличие в ней закладок;
- Q достоверно установлена неизменность BIOS и операционной системы для данного сеанса;

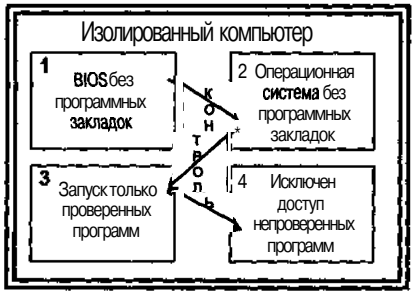


Рис. 3.37. Изолированный компьютер

О на компьютере не запускалось и не запускается никаких иных программ, кроме уже прошедших проверку на присутствие в них закладок;

- исключен запуск проверенных программ в каких-либо иных условиях, кроме перечисленных выше, т. е. вне изолированного компьютера.

Для определения степени изолированности компьютера может использоваться модель ступенчатого контроля. Суть ее заключается в следующем. Сначала производится проверка, нет ли изменений в BIOS. Затем, если все в порядке, считываются загрузочный сектор диска и драйверы операционной системы, которые, в свою очередь, также анализируются на предмет внесения в них несанкционированных изменений. И наконец, с помощью операционной системы запускается драйвер контроля вызовов программ, который следит за тем, чтобы в компьютере запускались только проверенные программы.

Программно-аппаратные методы защиты от удаленных атак

В настоящее время программно-аппаратные методы защиты от удаленных атак в сети Internet строятся на основе алгоритмов шифрования, практической реализацией которых являются криптопротоколы и межсетевые экраны (или брандмауэры).

При шифровании сетевых пакетов образуется так называемое защищенное соединение, главным элементом которого является криптопротокол. Для этих целей широко используются следующие протоколы криптографического шифрования:

- SKIP (Secure Key Internet Protocol);
- S-HTTP (Secure HTTP);
- a SSL (Secure Socket Layer).

SKIP-пакет — это обычный IP-пакет, поле данных которого представляет собой SKIP-заголовок определенного спецификацией формата и криптограмму (зашифрованные данные). Такая структура SKIP-пакета позволяет беспрепятственно направлять его любому хосту в сети Internet (межсетевая адресация происходит по обычному IP-заголовку в SKIP-пакете). Конечный получатель SKIP-пакета по заранее определенному разработчиками алгоритму расшифровывает криптограмму и формирует обычный TCP- или UDP-пакет, который и передает соответствующему обычному модулю (TCP или UDP) ядра операционной системы. В принципе, ничто не мешает разработчику формировать по данной схеме свой оригинальный заголовок, отличный от SKIP-заголовка.

Программный пакет S-HTTP — это защищенный HTTP-протокол, разработанный компанией Enterprise Integration Technologies (EIT) специально для Web. Этот протокол позволяет обеспечить надежную криптозащиту только HTTP-документов Web-севера. Эта особенность протокола S-HTTP делает его абсолютно специализированным средством защиты соединения, и, как следствие, невозможным его применение для защиты всех остальных прикладных протоколов (FTP, TELNET, SMTP и др.).

Протокол SSL — универсальный протокол защиты соединения, функционирующий на сеансовом уровне OSI, разработанный компанией Netscape. Данный протокол использует криптографию с открытым ключом и на сегодняшний день является, пожалуй, единственным универсальным средством, позволяющим динамически защитить любое соединение с использованием любого прикладного протокола (DNS, FTP, TELNET, SMTP и т. д.). Это связано с тем, что SSL, в отличие от S-HTTP, функционирует на промежуточном сеансовом уровне OSI (между транспортным — TCP, UDP и прикладным — FTP, TELNET и т. д.). В ходе соединения вырабатывается криптостойкий сеансовый ключ, используемый в дальнейшем абонентами SSL-соединения для шифрования передаваемых сообщений. Протокол SSL сегодня уже практически оформился в качестве официального стандарта защиты для HTTP-соединений, то есть для защиты Web-серверов. Большинство браузеров поддерживает этот протокол. Более того, под защищенным соединением в настоящее время все чаще понимается именно SSL.

Итак, очевидно, что повсеместное применение этих защищенных протоколов обмена, особенно SSL, способно поставить надежный барьер на пути всевозможных удаленных атак, прежде всего благодаря тому, что в случае использования криптографии становится бессмысленным перехват и анализ сетевого графика.

Однако пока ни один из существующих криптопротоколов (а их уже немало) не оформился в качестве единого стандарта защиты соединения, который поддерживали бы все производители сетевых операционных систем. С другой стороны, сдвиги в этом направлении все же имеются.

В настоящее время существуют несколько практических вариантов подключения корпоративных сетей к Internet:

- выделенный канал «точка- точка»;
- технология ISDN;
- технология Frame Relay.

Выделенный канал «точка- точка» предприятие может использовать для постоянного доступа в Internet (рис. 3.38, а). В этом канале применяется интерфейс V.35.

Технология ISDN используется, если у предприятие есть две цифровые коммутируемые линии (два B-канала): для телефонных переговоров и для работы в Internet в произвольной комбинации (рис. 3.38, б). Скорость каждого B-канала при выходе в Internet составляет 64 кбит/с (два B-канала — 128 кбит/с).

Технология Frame Relay применяется в том случае, когда предприятие пользуется высокоскоростным соединением с Internet на основе специального маршрутизатора (рис. 3.38, в). Скорость передачи данных колеблется между максимальной (64 кбит/с) и минимально гарантированной в зависимости от загруженности сети передачи данных.

Существенно, что все перечисленные варианты подключения корпоративной сети к Internet, обладая в стандартной конфигурации высокой производительностью, не могут обеспечить:

- безопасное взаимодействие пользователей и информационных ресурсов, расположенных в Extranet- и intranet-сетях, с Internet;
- технологически единый комплекс мер защиты для распределенных и сегментированных локальных сетей подразделений предприятия;

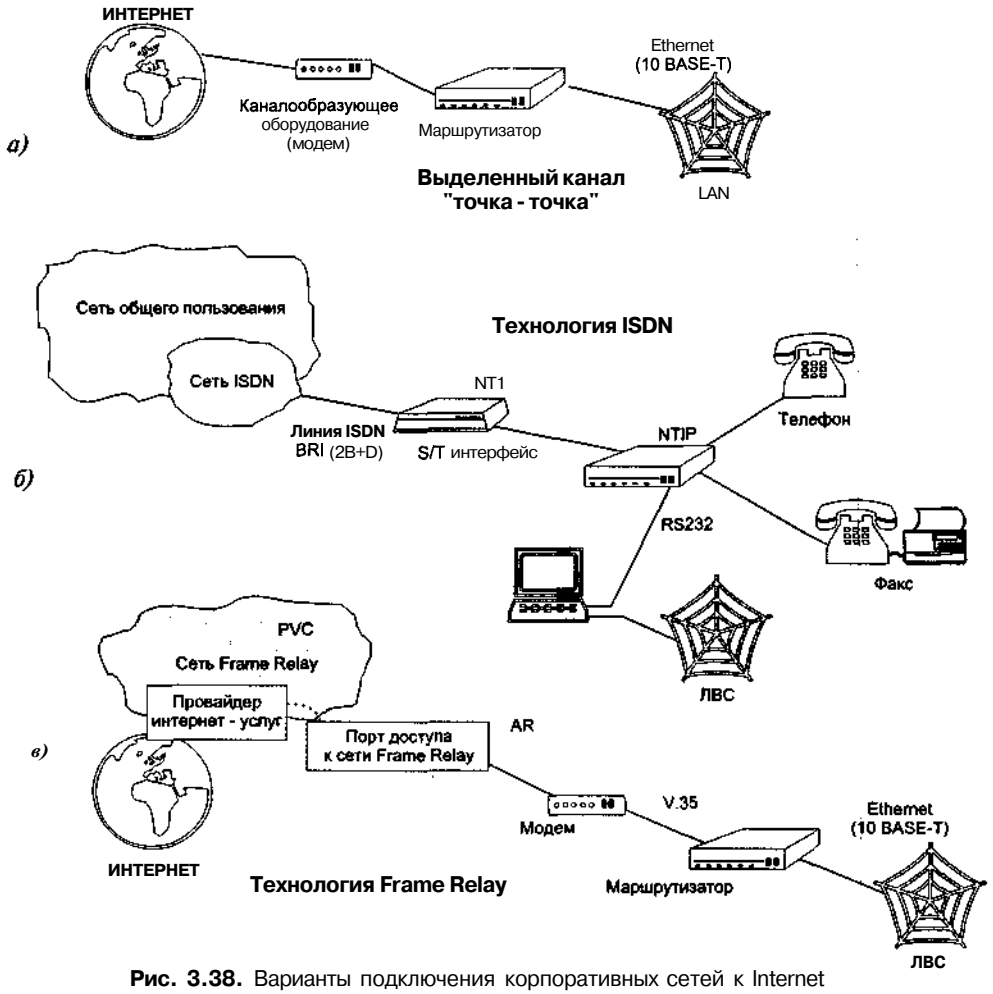


Рис. 3.38. Варианты подключения корпоративных сетей к Internet

- иерархическую систему защиты, предоставляющую адекватные средства обеспечения безопасности для различных по степени закрытости сегментов корпоративной сети.

Решить данные задачи становится возможным только при помощи технологии межсетевых экранов, организующей безопасное взаимодействие с внешней средой. Сравнительные характеристики возможных решений технологии межсетевых экранов (МЭ) приведены в табл. 3.8.

При подключении компьютерной сети к Internet рекомендуется защитить эту сеть от НСД с помощью одного из следующих решений на основе:

- аппаратно-программного или программного межсетевого экрана;
- маршрутизатора со встроенным пакетным фильтром;
- специализированного маршрутизатора, реализующего механизм защиты на основе списков доступа;

Таблица 3.8. Сравнительные характеристики возможных решений технологии межсетевых экранов

	Вариант подключения		
	Технология ISDN	Технология Frame Relay	Выделенный канал точка — точка
	Характеристика уровня защиты		
Защита на основе аппаратного firewall	Высокий	Высокий	Экономически не эффективно
Защита на основе программного межсетевого экрана	Высокий/средний (в зависимости от типа МЭ)	Высокий/средний (в зависимости от типа МЭ)	Высокий/ссредний (в зависимости от типа МЭ)
Защита на основе маршрутизатора с функциями firewall	Высокий/средний (в зависимости от типа маршрутизатора)	Высокий/средний (в зависимости от типа маршрутизатора)	Высокий
Защита на основе маршрутизатора	Низкий/средний (в зависимости от типа маршрутизатора)	Низкий/средний (в зависимости от типа маршрутизатора)	Средний

- операционной системы (ОС) семейства UNIX или реже MS Windows, усиленной специальными утилитами, реализующими пакетную фильтрацию.

Рассмотрим технологии межсетевого экранирования более подробно.

Прямую защиту корпоративной системы предоставляет методика, так называемая «огненная стена» (Firewall). По этой методике в сети выделяется определенная буферная область, и далее все сетевые пакеты между локальной сетью и Internet проходят только через этот буфер.

Защита корпоративной сети на основе Firewall позволяет получить максимальную степень безопасности и реализовать следующие возможности:

- семантическую фильтрацию циркулирующих потоков данных;
- фильтрацию на основе сетевых адресов отправителя и получателя;
- фильтрацию запросов на транспортном уровне на установление виртуальных соединений;
- фильтрацию запросов на прикладном уровне к прикладным сервисам;
- локальную сигнализацию попыток нарушения правил фильтрации;
- запрет доступа неизвестного субъекта или субъекта, подлинность которого при аутентификации не подтвердилась, и др.;
- О обеспечение безопасности от точки до точки: межсетевой экран, авторизация маршрута и маршрутизатора, тоннель для маршрута и криптозащита данных;
- многопротокольную маршрутизацию (IP, IPX, AppleTalk) и прозрачный мост через ISDN, асинхронное и синхронное, последовательное соединение, такое как выделенная линия. Frame Relay, SMDS, Switched 56 и X.25;
- возможность обеспечения качества услуги от точки до точки посредством протокола резервирования ресурсов (RSVP), очереди с весами (WFQ), IP Multicast и AppleTalk Simple Multicast Routing Protocol (SMRP) для обеспечения таких приложений, как видеоконференции, объединение данных и голоса и др.;

- расширенный доступ к Internet/Intranet (трансляция сетевых адресов (NAT), IPeXchange шлюз IP-B-IP, простота и снижение стоимости доступа к Internet и Intranet);
- оптимизацию WAN (установление соединения по требованию (DDR), предоставление полосы по требованию (BOD) и OSPF по требованию, полустатическая маршрутизация, сжатие и фильтрация).

Существенно, что только выделенные межсетевые экраны позволяют осуществить комплексную зачету корпоративной сети от НСД, основанную как на традиционной синтаксической (IP-пакетной) фильтрации контролируемых потоков данных, осуществляемой большинством операционных систем семейств Windows и UNIX, так и на семантической, доступной только коммерческим специальным решениям.

В настоящее время все известные Firewall можно разделить на несколько основных групп:

- по исполнению:
- G аппаратно-программный;
- O программный;
- G по функционированию на уровнях модели OSI:
- шлюз экспертного уровня;
- экранирующий шлюз (прикладной шлюз);
- экранирующий транспорт (шлюз сеансового уровня);
- экранирующий маршрутизатор (пакетный фильтр);
- по используемой технологии:
- stateful inspection (контроль состояния протокола);
- O на основе модулей-посредников (proxy);
- по схеме подключения:
- схема единой защиты сети;
- схема с защищаемым закрытым и не защищаемым открытым сегментами сети;
- схема с раздельной защитой закрытого и открытого сегментов сети.

Пример программно-аппаратной реализации такой стратегии Firewall — межсетевой экран.

Межсетевой экран — система (или комбинация систем), позволяющая разделить сеть на две или более частей и реализовать набор правил, определяющих условия прохождения пакетов из одной части в другую. Как правило, эта граница проводится между корпоративной сетью и Internet, хотя ее можно провести и внутри локальной сети. Таким образом, межсетевой экран пропускает через себя весь трафик. Он принимает решение, пропускать пакет или отбросить. Решение производится опять-таки на основании определенных правил, как и в случае чисто административного управления. Однако правила задаются уже не только на программном, но и на аппаратном уровне, что существенно затрудняет взлом подобных систем.

Необходимо отметить, что в настоящее время наряду с одноуровневыми межсетевыми экранами все большую популярность приобретают комплексные экраны, охватывающие уровни от сетевого до прикладного.

Конкретные реализации межсетевых экранов в значительной степени зависят от используемых вычислительных платформ, но, тем не менее, все системы этого класса используют два механизма, один из которых обеспечивает блокировку сетевого трафика, а

второй, наоборот, разрешает обмен данными. При этом некоторые версии межсетевых экранов делают упор на блокировании нежелательного трафика, а другие — на регламентировании разрешенного межмашинного обмена. Возможный вариант защиты сети на основе аппаратно-программного межсетевого экрана представлен на рис. 3.39.

Поскольку межсетевые экраны ориентированы на защиту информации в открытых сетях типа Intemel/intranet, основой подхода служит семиуровневая модель ISO/OSI (Международной организации по стандартизации). В соответствии с этой моделью межсетевые экраны классифицируются по тому, на каком уровне происходит фильтрация: канальном, сетевом, транспортном, сеансовом или прикладном. Поэтому можно говорить об экранирующих концентраторах (канальный уровень), маршрутизаторах (сетевой уровень), транспортном экранировании (транспортный уровень), шлюзах сеансового уровня (сеансовый уровень) и прикладных экранах (прикладной уровень).

Еще одним важным компонентом межсетевого экрана является система сбора статистики и предупреждения об атаке (так называемый аудит). Информация обо всех событиях (отказах, входящих, выходящих соединениях, числе переданных байт, использовавшихся сервисах, времени соединения и т. д.) накапливается в файлах статистики.

Упрощенно все межсетевые экраны можно разбить на две группы:

- фильтры пакетов;
- шлюзы приложений.

В основе функционирования фильтров пакетов лежит привязанность отдельных служб Internet к портам: например, WWW-соединения обычно используют порт 80. Для фильтрации пакетов, помимо номеров портов, нужны также IP-адреса задействованных компьютеров. Большинство существующих сегодня маршрутизаторов предлагают такой сервис. Современные продукты развития фильтров пакетов также позволяют анализировать статус соединения. Они различают вновь устанавливаемое и уже существующее соединения и при этом держат в памяти короткую историю прохождения предыдущих блоков данных. Однако содержимое пакетов не поддается исследованию с помощью фильтров, т. к. последние не понимают, например, протоколов HTTP и FTP.

Защита на основе маршрутизатора со встроенным пакетным Firewall характеризуется высокой эффективностью и безопасностью. В настоящее время одним из наиболее интересных является вариант защиты на основе маршрутизаторов Cisco 1720 (рис. 3.40).

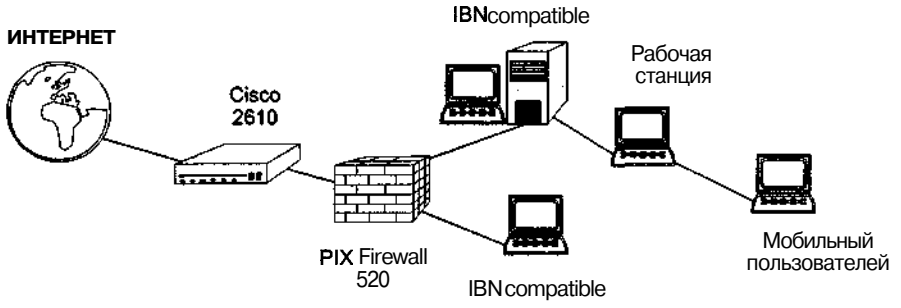


Рис. 3.39. Возможный вариант защиты сети на основе аппаратно-программного межсетевого экрана

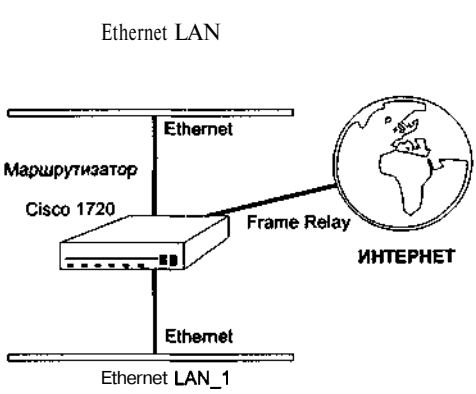


Рис. 3.40. Вариант защиты на основе маршрутизаторов со встроенным пакетным Firewall

Рассматриваемое решение основано на использовании маршрутизатора Cisco 1720 компании Cisco Systems. Высокая производительность маршрутизатора основана на схеме пакетной фильтрации и возможности установки дополнительной защиты, реализованной на основе firewall features. Этот вариант обладает следующими достоинствами:

О высокая производительность и пропускная способность;

- преимущества пакетного и прикладного шлюзов;
- простота и надежность в эксплуатации и установке;

О возможностью обеспечения безопасности от точки до точки: межсетевой экран, авторизация маршрута и маршрутизатора, тоннель для маршрута и криптозащита данных;

- многопротокольная маршрутизация (IP, IPX, AppleTalk) и прозрачный мост через ISDN, асинхронное и синхронное, последовательное соединение, такое как выделенная линия, Frame Relay, SMDS, Switched 56 и X.25;
- возможность обеспечения качества услуги от точки до точки посредством протокола резервирования ресурсов (RSVP), очереди с весами (WFQ), IP Multicast и AppleTalk Simple Multicast Routing Protocol (SMRP) для обеспечения таких приложений, как видеоконференции, объединение данных и голоса и др.;
- расширенные возможности доступа к Internet/intranet (трансляция сетевых адресов (NAT), IPeXchange шлюз ipx-b-ip, простота и снижение стоимости доступа к Internet и intranet);;
- возможность оптимизации WAN (установление соединения по требованию (DDR), предоставление полосы по требованию (BOD) и OSPF по требованию, полустатическая маршрутизация, сжатие и фильтрация).

Другой рассматриваемый вариант защиты основывается на использовании специализированного маршрутизатора с листами доступа. Он самый распространенный на сегодняшний день (рис. 3.41). В нем наиболее интересным решением является использование маршрутизаторов компании Cisco Systems, например Cisco 1750 и серии 2600 — Cisco 2610.

Данный вариант обладает высокой эффективностью и достаточной безопасностью. Основные преимущества такого решения заключаются в гибкости, мультисервисном доступе, защите инвестиций.

Для подключения сети предприятия к Internet можно использовать все существующие серии маршрутизаторов Cisco.

Еще один способ защиты основывается на операционных системах семейств UNIX Windows, усиленных функцией пакетной фильтрации. В данном случае системное программное обеспечение выполняет функции маршрутизации, фильтрации, сервисного обслуживания и др. По уровню надежности, безопасности и производительности

наиболее предпочтительны решения на основе UNIX-подобной операционной системы (например, Solaris, BSD/OS 4.0 или Linux).

Шлюзы приложений контролируют содержимое пакетов данных на уровне приложений. Они способны проверять программы на наличие вирусов или удалять с Web-страниц активное содержимое, например, Java-апплеты или элементы управления ActiveX. При этом для отдельных служб требуются proxy-процессы, пересылающие запросы от компьютеров в локальной сети на Internet-сервер и проверяющие пакеты данных. Поскольку анализ трафика между Internet и локальной сетью требует определенных вычислительных ресурсов, решение этих задач должен взять на себя соответствующим образом оборудованный компьютер. В отличие от пакетных фильтров, шлюзы приложений позволяют ограничить количество допустимых операций за одно соединение.

Чтобы при выходе из строя одного из компонентов обезопасить локальную сеть от вторжений, рекомендуется создавать многоступенчатую систему межсетевых экранов. Целесообразно использовать шлюз приложений, снабженный дополнительной защитой в виде двух фильтров пакетов: одного — на входе в корпоративную сеть со стороны Internet, а другого — на ее выходе в Internet.

Симметричное построение обеспечивает также определенную защиту от несанкционированных действий в собственной сети компании. При этом Internet-сервер следует подключать к одной или нескольким сетевым платам таким образом, чтобы он был защищен шлюзом приложений и вместе с тем не находился бы непосредственно в локальной сети. Он имеет право общаться с внутренней сетью лишь через шлюз приложений и внутренние фильтры пакетов.

С другой стороны, безопасность данных не есть что-то застывшее. Одно лишь приобретение и рациональное конфигурирование подходящего межсетевого экрана не означает, что риск вторжений из Internet в корпоративную сеть исключен надолго. Помимо регулярного и, по возможности, оперативного контроля протокольных данных, администраторы должны неустанно следить за возникающими прорехами в системе безопасности и узнавать о новых сценариях вторжений извне, чтобы своевременно сделать в системе соответствующие «заплатки». Компаниям необходимо

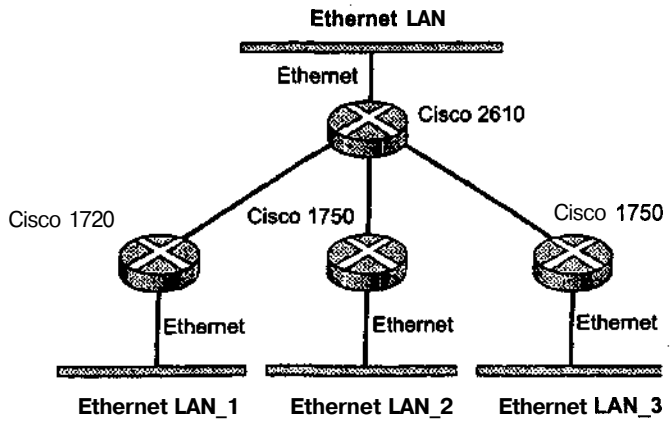


Рис. 3.41. Вариант защиты на основе маршрутизаторов с листами доступа

периодически пересматривать планы мероприятий, направленные на защиту данных, а также конфигурацию межсетевого экрана.

Недостатки межсетевых экранов — их достаточно высокая стоимость и сложность в настройке. Зато они дают довольно высокую степень безопасности и позволяют современно выявлять не только атаки, но и попытки несанкционированного воздействия на корпоративную сеть. Сравнительные характеристики некоторых межсетевых экранов представлены в табл. 3.9.

Таблица 3.9. Сравнительные характеристики некоторых межсетевых экранов

Наименование продукта	Cisco PIX 520 (506,525,535)	Checkpoint Firewall-1	Застава	Raptor Symantec-AXENT	CyberWall-PLUS
Поставщик Производитель	Cisco Systems	Check Point	Элвис+	Symantec-AXENT	Network-1
Класс Гостехкомиссии России	3, разовая сертификация (для Cisco PIX 520)	3 (сертификат на серию)	3 (сертификат на серию)	Нет	(4) Готовится к сертификации по
Используемая ОС (платформа)	ОС собственной разработки	Solaris (SPARC), NT (x86), HP-UX (HP)	Solaris (SPARC)	Solaris (SPARC), NT (x86), HP-UX (HP)	NT2000 (x86)
Уровень фильтрации	Сеансовый, сетевой	Прикладной, сеансовый, сетевой	Прикладной, сеансовый, сетевой	Прикладной, сеансовый, сетевой	Прикладной, сеансовый, сетевой
Прозрачность для приложений	Прозрачен	Прозрачен	Прозрачен	Прозрачен	Прозрачен
Proxy	нет	нет	нет	Http,ftp, telnet, riogin, rsh, smtp, snmp, POP3,gopher, SSL, XI 1, SQL, Ip, nntp, RealAudio, ReatVideo, StreamWorks.VOOlive, NetShow, LDAP	http, ftp, RealAudio
Поддержка протоколов для фильтрации	ftp, SMTP, archie, gopher, telnet,H.323, NetMeeting, InternetPhone, RealAudio	FTP,RPC, H.323, NetMeeting, VDOLive, NetShow, CU-SeeMe, MS Exchange, RealAudio, SQLNet,Vosaic, WebTheater.Win Frame	rsh,smtp,snrnp, POP3, gopher, SSL, XI I.SQL, Ip, nntp, RealAudio, RealVideo, StreamWorks.V DOlive, NetShow, LDAP	FTP,RPC,H.323, NetMeeting, VDOLive, NetShow, CU-SeeMe, MS Exchange, RealAudio, SQLNel,Vosaic, WebTheater, WinFrame	Более 1000 протоколов
Трансляция сетевых адресов	Есть	Есть	Есть	Есть	Есть
Аутентификация пользователей	Secure, RADIUS, TACACS+.AXENT, CryptoCard	S/Key.SecurIO, RADIUS, TACACS, TACACS+, Definder, OSPassword	RADIUS	S/Key, SecurID, RADIUS, TACACS, TACACS+, Definder, OSPassword	S/Key, SecurID, RADIUS

Продолжение табл. 3.9

Генерация отчетов	Текст	Бинарный формат	Текст	Текст	Текст, бинарный формат
Аутентифицируемые протоколы	ftp, http, telnet	Все	Pop3	Все	ftp, http, telnet, riogin
Реагирование на попытки НСД	Есть	Есть	Есть	Есть	Есть
Централизованное администрирование	Есть	Есть (отдельная утилита)	Нет	Есть	Есть
Предельная производительн	1 Гбит/с	100 Мбит/с	10 Мбит/с	100 Мбит/с	100 Мбит/с
Контекстный просмотр кода Java/ActiveX	Да	Да	Нет	Да	Да
Поддержка технологии Plug-and-Play	Есть	Невозможно	Нет	Есть	Есть
Лицензирование	По количеству соединений (от 64 000 до 256 000 и выше)	На 25,50,250,500 клиентов и unlimited	На 50,100 IP и unlimited	На 25,50,250,500 клиентов и unlimited	На рабочие станции - 10,100, 250 клиентов. На корпоративные серверы — 1, 5,10,15 серверов. На всю сеть — 100,500 сессий и unlimited

Рассмотрим возможные решения по организации безопасного подключения корпоративной сети к Internet.

В современных условиях более 50% различных атак и попыток доступа к информации осуществляется изнутри локальных сетей, в связи с чем классический «периметровый» подход к созданию системы защиты корпоративной сети становится недостаточно эффективным. О действительно защищенной от НСД сети можно говорить только при наличии в ней как средств защиты точек входа со стороны Internet, так и решений, обеспечивающих безопасность отдельных компьютеров, корпоративных серверов и фрагментов локальной сети предприятия. Последнее наилучшим образом обеспечивают решения на основе распределенных или персональных межсетевых экранов.

Внутренние корпоративные серверы компании, как правило, представляют собой приложения под управлением операционной системы Windows NT/2000, Netware или, реже, семейства UNIX, например, Linux или BSD 4.0/4.1. По этой причине корпоративные серверы становятся потенциально уязвимыми для различного рода атак. Так, например, широко распространенные серверы под управлением операционной системы Windows NT/2000 находятся выше стека протоколов сервера NT. Между тем, данная операционная система не проводит мониторинг и регистрацию событий в сети, не выявляет подозрительную активность в ней и не блокирует множество входящих и исходя-

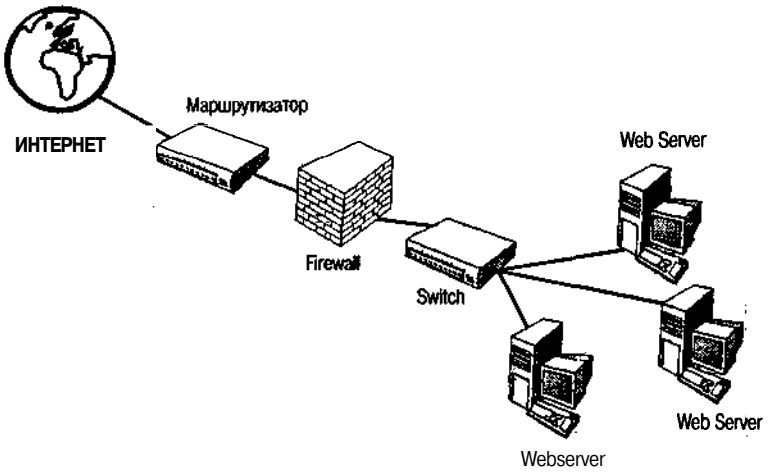


Рис. 3.42. Классическая схема защиты корпоративных серверов

щих соединений. Из-за недостатка функций контроля доступа и обнаружения вторжений становятся открытыми операционные системы корпоративных серверов, а соответственно и их приложения, для различного рода атак, например, DoS-атак (Ping Flood, SYN Flood, IP Packet Fragmentation, TCP and UDP Port Spooring, Session Highjacking, Oversized IP Packet Attacks), а также внедрения троянских коней и подбора пароля.

Даже если сервер компании защищен стандартными средствами, это не предотвратит попытки нарушения безопасности самой операционной системы. Если атакующий, используя DoS-атаку, блокирует сервер, автоматически блокируется и приложение. Как результат, компания несет убытки, связанные с нарушением работоспособности своей сети. Именно поэтому рассмотрим способы использующихся специальных защитных механизмов защиты серверов.

Простейшим классическим способом защиты внутренних серверов компании от внешних атак является установка Firewall, например, Firewall-1 компании Checkpoint или Cisco PIX компании Cisco, между серверами и Internet (рис. 3.42).

При правильной конфигурации большинство Firewall могут защитить внутренние серверы от внешних злоумышленников, а некоторые из них могут даже выявлять и предотвращать атаки типа «отказ в обслуживании». Тем не менее, этот подход не лишен некоторых недостатков.

Когда корпоративные серверы защищены одним-единственным межсетевым экраном, все правила контроля доступа и все верифицированные данные оказываются сосредоточенными в одном месте. Таким образом, Firewall становится «узким местом» и по мере возрастания нагрузки значительно снижается его производительность. Конечно, Firewall можно дополнить программным обеспечением, балансирующим нагрузку (например, FloodGate компании Checkpoint) и многопроцессорными модулями, но эти шаги только усложнят систему и повысят ее стоимость.

Альтернативой классической схеме является схема децентрализованной защиты корпоративных серверов, основанная на установке продукта Firewall-1 компании Checkpoint или Cisco PIX компании Cisco перед каждым сервером (рис. 3.43). В результате того, что

Firewall становится выделенным ресурсом сервера, решается проблема «узкого места» и уменьшается влияние отказа отдельного межсетевого экрана на общее состояние сети.

Однако и данный подход не лишен существенных недостатков. Система из десяти серверов потребовала бы десяти лицензированных конфигураций Firewall, работающих на десяти аппаратных платформах с десятью операционными системами, требующими администрирования и обслуживания. Соответственно, на порядок возрастают величина издержек, сложность администрирования и частота отказов. Даже если учесть, что влияние отказа отдельного Firewall сокращается в результате демонтажа лишь одной системы вместо десяти, среднее время наработки на отказ для десяти продуктов firewall оказывается в десять раз хуже, чем для одного. Например, если в сервере происходит отказ аппаратного обеспечения, в среднем, один раз в двадцать месяцев, то при использовании десяти серверов этот промежуток времени сократится до двух.

Наиболее подходящим решением этой проблемы является размещение средств безопасности на одной платформе с сервером, который они будут защищать. Эта задача решается путем использования распределенных или персональных межсетевых экранов, например, CyberwallPLUS компании Network-1 (рис. 3.44).

Данные решения существенно дополняют функциональные возможности традиционных (периметровых) экранов и могут использоваться для защиты как внутренних, так и Internet-серверов.

В отличие от традиционных продуктов Firewall, как правило, представляющих собой локальные «контрольные точки» контроля доступа к критическим информационным ресурсам корпорации, распределенные межсетевые экраны — это дополнительное программное обеспечение, которое защищает корпоративные сервера, например Internet-сервер. Сравним традиционный и распределенный межсетевые экраны по таким показателям, как:

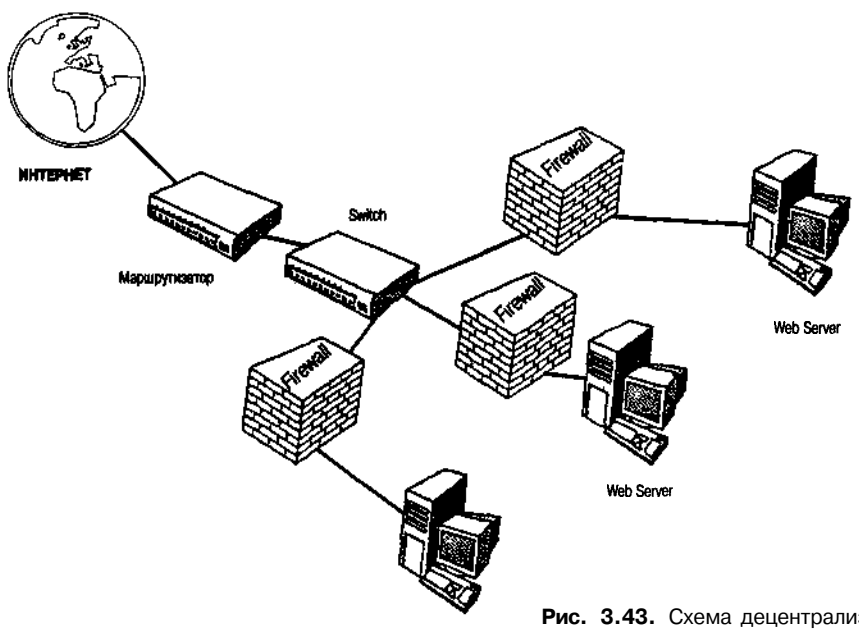


Рис. 3.43. Схема децентрализованной защиты корпоративных серверов

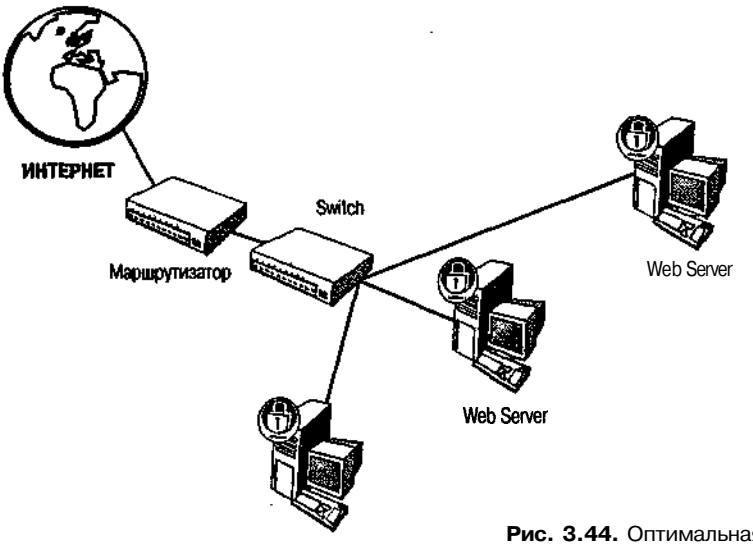


Рис. 3.44. Оптимальная схема защиты корпоративных серверов

- ❑ эффективность;
- ❑ простота установки;
- ❑ управление;
- ❑ производительность;
- О стоимость.

Результаты сравнения представлены в табл. 3.10.

Технология распределенных экранов появилась сравнительно недавно. Поэтому, чтобы более детально разобраться с работой и преимуществами данной технологии, рассмотрим одно из возможных решений.

Возьмем для примера межсетевые экраны CyberwallPLUS. Эти межсетевые экраны сочетают в себе средства контроля сетевого доступа со встроенными средствами выявления несанкционированного доступа. Они работают в режиме ядра, проверяя каждый пакет информации по мере его поступления из сети. Несанкционированные действия, такие как попытки взлома и несанкционированного доступа, блокируются до перехода на уровень приложений сервера.

Основные преимущества распределенных Firewall для защиты Internet-серверов следующие:

- G обеспечение безопасности входящего и исходящего графика на всех NIC, закрепленных за сервером;
- ❑ обеспечение масштабируемой архитектуры путем распространения безопасности Firewall на многочисленные серверы;
- ❑ устранение традиционного продукта Firewall как единственного места сбоев;
- О обеспечение недорогого, легкого в реализации и управлении решения безопасности (программное обеспечение сервера в сравнении с сетевым аппаратным обеспечением).

Важно, что межсетевой экран CyberwallPlus-SV использует уникальную структуру безопасности и, обеспечивая присутствие двух ее ключевых элементов (функций

Таблица 3.10. Сравнительные характеристики традиционных и распределенных межсетевых экранов

Вид экрана	Характеристика				
	Эффективность	Простота установки	Управление	Производительность	Стоимость
Традиционный	Часто располагается по периметру сети, обеспечивая лишь один слой защиты. И если этот единственный слой нарушен, система оказывается незащищенной перед любыми атаками	Устанавливается как часть конфигурации корпоративной сети	Управляется сетевым администратором	Является устройством обеспечения межсетевого обмена с фиксированным ограничением производительности по пакетам в секунду. Он не подходит для растущих серверных парков, соединенных между собой коммутированными местными сетями	Являются, как правило, системами с фиксированными функциями и достаточно высокой стоимостью (примерно от $ 4500)
Распределенный	Функционирует на уровне ядра операционной системы и надежно защищает корпоративные сервера, проверяя все входящие и исходящие пакеты	Представляет собой программное обеспечение, которое устанавливается и удаляется в считанные минуты	Может управляться либо сетевым администратором, либо пользователем локальной сети	Позволяет производить наращивание серверных парков без ущерба принятой политике безопасности. Несмотря на то что встроенный Firewall в определенной мере загружается с центрального процессора хоста, обработка правил безопасности распространяется на всех участников серверного парка, допуская неограниченный рост сети	Представляет собой программное обеспечение, которое стоит, как правило, от 1/5 до 1/10 цены традиционных экранов

контроля доступа к ресурсам сети и активного обнаружения вторжений), защищает операционную систему Windows NT от попыток нарушения защиты.

Ядро безопасности экрана CyberwallPlus-SV расположено между сетевой картой сервера и стеком протоколов — ниже, чем защищаемые приложения.

Для обеспечения безопасности NT-приложений, таких как корпоративные серверы, рекомендуется защитить доступ к ним через операционную систему. CyberwallPlus-SV позволяет закрыть все неиспользуемые порты, тем самым ограничивая доступ к NT-приложениям и сервисам. Те или иные сервисы могут иметь специфические сетевые адреса для направления (входящий/исходящий) и для времени (дата, время Windows), которые задают базу правил контроля доступа.

Межсетевой экран CyberwallPlus-SV также обеспечивает активное обнаружение вторжений для NT-системы, защищая ее от атак и сканирования. Наиболее легким путем негативного воздействия на Internet-сервер является блокирование NT-сервера, на котором находится приложение. Обычно это делается посредством DoS-атаки, при которой поток пакетов, отправленных серверу, перегружает память и нарушает работоспособность системы. Также примером нарушения защиты являются атаки типа Ping Flood и SYN Flood.

Другой способ нарушения защиты Internet-сервера — сканирование NT-сервера на наличие открытого порта или «backdoor». Обычно это называется сканированием TCP- или UDP-портов.

CyberwallPlus-SV предотвращает DoS-атаки и сканирование портов, конфигурируя систему безопасности: например, ограничивая число обращений к серверу за некото-

рый отрезок времени. Установки также определяют количество портов, которые могут быть использованы (опробованы) в течение определенного отрезка времени. Если эти условия нарушаются, CyberwallPtus-SV может прервать соединение, записать нарушение и сообщить о нем администратору по электронное почте. В результате доступ к корпоративным серверам для различного рода злоумышленников надежно блокируется.

Таким образом, межсетевые экраны CyberwallPlus обеспечивают дополнительный уровень защиты платформ под управлением операционной системы Windows NT/2000, на которых установлены корпоративные приложения, например Internet-сервер. Кроме того, CyberwallPlus-SV может также предотвратить применение атак известных типов для вторжений на критичные серверы компании и сообщить администратору безопасности о подозрительной деятельности в сети.

ГЛАВА 4. КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Криптографические методы традиционно используются для шифрования конфиденциальной информации, представленной в любой материальной форме в виде:

- письменных текстов;
- данных, хранящихся на гибком диске;
- сообщений, передаваемых в телекоммуникационных сетях;
- программного обеспечения, графики или речи, закодированных цифровыми последовательностями и т. п.

Эти методы могут быть использованы и для многих других приложений, связанных с защитой информации, в частности, для обнаружения фактов вторжения в телекоммуникационную или компьютерную сеть и введения в нее имитирующих сообщений. В настоящее время криптографическое преобразование информации в форму, непонятную для посторонних, является универсальным и надежным способом ее защиты.

Проблема защиты информации путем ее преобразования, исключающего ее прочтение посторонним лицом, волновала человеческий ум с давних времен. Поэтому сделаем небольшой экскурс в историю. Рассмотрим лишь небольшой отрезок времени и посмотрим, что и как шифровали раньше.

История применения криптографических методов насчитывает десятки веков. Упоминания о криптографии (от греч. kryptos — скрытый, тайный) встречаются еще у Геродота и Плутарха, а также в русских рукописях XII—XIII веков. Но криптография появилась гораздо раньше — она ровесница истории человеческого языка.

Одной из важнейших способностей человека является умение общаться с себе подобными. Изначально для передачи сведений о том, что происходит в окружающем мире, о фактах своей субъективной реальности, человек использовал жесты и мимику.

Язык тайной передачи сообщений жестами активно используется и в наши дни представителями некоторых криминальных «специальностей», например, шулеров. Во время «работы» пара шулеров ведет весьма оживленную беседу, незаметную для непосвященных и понятную только наметанному глазу профессионала.

Тема передачи сообщений посредством условных знаков или жестов активно используется писателями и сценаристами приключенческого жанра. Вспомните фильмы и книги о войне: цветок на окне, поднятая или опущенная занавеска, объявление с условной фразой в газете, выбор цветов во время покупки их у цветочника-связника и т. д.

С развитием речи — второй сигнальной системы человека, которая по праву считается одним из важнейших отличительных признаков, качественно выделяющих чело-

вещество из животного мира, — информационный обмен между членами даже самого дикого племени многократно усложнился. Люди стали разговаривать с кем-то больше, с кем-то меньше, ведь коммуникация в человеческом обществе имеет еще один отличительный признак — она узко избирательна. Разговаривая с разными людьми, мы ведем себя совершенно по-разному: то, что сообщаем одним, стараемся скрыть от других.

Как видим, уже с самого зарождения человеческой цивилизации люди научились сообщать информацию так, чтобы она стала известна одним людям и не была известна другим. Пока для передачи сообщений использовались исключительно голос и жесты, сделать это не составляло особого труда: нужно было всего лишь исключить присутствие в непосредственной близости от разговаривающих тех людей, для которых сообщаемые сведения не были предназначены. Однако иногда собеседники не могли скрыться от посторонних ушей и глаз. Для обмена информацией в подобных обстоятельствах была создана (а точнее, сложилась сама собой) система сообщений, кодированных речью или жестами. В различных ситуациях она носила совершенно различный характер — от отдельного тайного знака, говорящего о наступлении определенного события, до развитых секретных языков, позволявших выражать практически любые мысли. Даже в самом простейшем случае это была, по сути своей, вторая сигнальная система в миниатюре, предназначенная для передачи ограниченного набора сведений и известная, как правило, лишь небольшой группе посвященных. Это был альтернативный язык общения, который и положил начало развившемуся позже искусству секретно передавать сообщения.

Конечно же, использование развитого «секретного» языка для защиты передаваемых данных обеспечивает гораздо большую свободу общения, чем несколько тайных знаков, о которых участники договорились заранее, однако и этот путь имеет свои недостатки. Трудно уследить за всеми, знающими «секретный» язык, и рано или поздно он станет понятным тому, от кого пытаются скрыть разговор. В этом случае возникнет необходимость заменить его другим. Но разработать достаточно мощный язык и обучить ему нужное количество людей трудно и накладно, а сделать это оперативно — практически невозможно. Поэтому подобный подход к проблеме проходит только в особых случаях, когда тому благоприятствуют обстоятельства. Так, он использовался американцами во время второй мировой войны: корабли ВМФ США осуществляли связь на языке малочисленного и компактно проживающего индейского племени. На каждом корабле было несколько индейцев-шифровальщиков; у противника не было почти никаких шансов заполучить себе такую «ходячую шифровальную машину».

С развитием письменности задача обеспечения секретности и подлинности передаваемых сообщений стала особенно актуальной. Действительно, сообщение, переданное словесно или показанное жестами, доступно для постороннего только в тот краткий промежуток времени, пока оно находилось «в пути», а в его авторстве и подлинности у получателя не может быть никаких сомнений, потому что он видит своего собеседника. Иное дело, когда сообщение записано. В этом случае оно уже живет отдельной жизнью и имеет свой путь. Сообщение, записанное на каком-либо носителе, существует в материальном мире, и у людей, желающих ознакомиться с его содержанием против воли отправителя и получателя, появляется гораздо больше шансов это сделать. Поэтому именно после возникновения письменности появилось искусст-

во тайнописи — набор методов, предназначенных для секретной передачи записанных сообщений от одного человека другому.

Более того, первоначально письменность сама по себе была криптографической системой, так как в древних обществах ею владели только избранные. Тому примеры — священные книги Древнего Египта, Древней Индии. Историки хорошо знают, что уникальные древние рукописные тексты, как правило, допускают неоднозначные трактовки, а часто и вообще не могут быть разумно интерпретированы современными учеными. И только массовые тиражи идентичных печатных текстов более поздних времен позволяют им достоверно говорить об однозначном восстановлении смысла информации, закодированной в этих текстах. Посмотрите на детские рисунки. Они тоже могут содержать некоторый текст (рис. 4.1).

С широким распространением письменности криптография стала формироваться как самостоятельная наука. Данные о первых способах тайнописи весьма обрывочны. Предполагается, что она была известна в Древнем Египте и Вавилоне. До нашего времени дошли сведения о том, что искусство секретного письма использовалось в Древней Греции. Первые действительно достоверные данные с описанием метода шифрования относятся к периоду смены старой и новой эры и описывают шифр Цезаря — способ, которым Юлий Цезарь прятал свои записи от излишне любопытных глаз. С высоты достижений современной криптографии шифр Цезаря предельно примитивен: в нем каждая буква сообщения заменялась на третью следующую за ней в алфавитном порядке букву. Однако для того времени, когда умение читать и писать было редким исключением, его криптостойкости вполне хватало.

Уже тогда использование шифра решало проблему секретности передаваемого сообщения, а проблема его подлинности решалась практически сама собой:

- человек, не знавший шифр, не мог внести осмысленные изменения в зашифрованные текстовые сообщения, а изменения, внесенные наобум, приводили к тому, что после расшифровки получался бессмысленный набор букв;
- поскольку отправляемые сообщения записывали от руки, то запомнить почерк каждого из нескольких десятков наиболее важных своих корреспондентов не составляло особого труда.

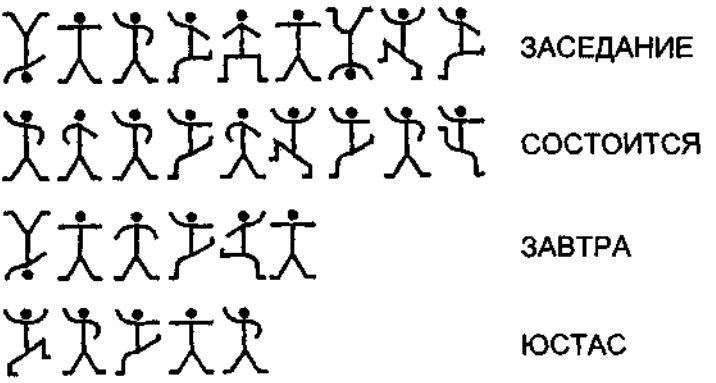


Рис. 4.1. Шифр «Пляшущие человечки»

Но проходили годы, и переписка, как средство общения, стала неотъемлемой частью процесса передачи информации. Чем оживленнее велась переписка в обществе, тем больше ощущалась потребность в средствах ее засекречивания. Соответственно, возникали все более совершенные и хитроумные шифры. Сначала появились шифровальщики, потом группы из нескольких шифровальщиков, а затем и целые шифровальные отделы. Когда объемы подлежащей закрытию информации, стали критическими, были созданы механические устройства для шифрования. Основными потребителями криптографических услуг стали дипломатические и шпионские миссии, тайные канцелярии правителей и штабы войсковых соединений. Для этого этапа развития криптографии характерно следующее:

- защите подвергались исключительно текстовые сообщения, написанные на естественных языках (других типов данных в то время просто не существовало);
- использовавшиеся шифры были достаточно простыми (шифрование сначала осуществлялось вручную, позднее были изобретены сравнительно несложные механические приспособления);
- научный подход к построению шифров и их раскрытию отсутствовал (криптография и криптоанализ были скорее искусством, чем наукой);
- криптографию использовали только высшие правящие слои и военная верхушка государств;
- основной задачей криптографии являлась защита передаваемых сообщений от несанкционированного ознакомления (поскольку шифровали исключительно текстовые сообщения, то никаких дополнительных методов защиты от навязывания ложных данных не применялось, т. к. в силу огромной избыточности, характерной для естественных языков, была ничтожно мала вероятность получить нечто осмысленное после расшифровки искаженного зашифрованного текста).

Особенно бурно криптографические системы развивались в годы первой и второй мировых войн. Благодаря вычислительным средствам ускорились разработка и совершенствование криптографических методов. Именно появление в середине прошлого столетия первых электронно-вычислительных машин кардинально изменило ситуацию.

С проникновением компьютеров в различные сферы жизни возникла принципиально новая отрасль — информационная индустрия. Объем циркулирующей в обществе информации примерно удваивается каждые пять лет. Человечество создало информационную цивилизацию, в которой от успешной работы средств обработки информации зависит само благополучие и даже выживание человечества в его нынешнем качестве. Произошедшие за этот период изменения можно охарактеризовать следующим образом:

- объемы обрабатываемой информации возросли за последние полвека на несколько порядков;
- информация приобрела стоимость, которую во многих случаях даже невозможно подсчитать;
- доступ к определенным данным позволяет контролировать значительные материальные и финансовые ценности;
- обрабатываемые данные стали чрезвычайно многообразными, а не исключительно текстовыми;

- информация полностью «обезличилась», т. е. особенности ее материального представления потеряли свое значение;
- характер информационных взаимодействий чрезвычайно усложнился (наряду с классической задачей защиты передаваемых текстовых сообщений от несанкционированного прочтения и их искажения возникли новые задачи защиты информации, ранее стоявшие и решавшиеся в рамках используемых «бумажных» технологий);
- субъектами информационных процессов теперь являются не только люди, но и созданные ими автоматические системы, действующие по заложенной в них программе;
- вычислительные возможности современных компьютеров подняли на совершенно новый уровень как возможности по реализации шифров, ранее немыслимых из-за своей сложности, так и возможности аналитиков по их взлому.

С появлением компьютеров и использованием для связи компьютерных сетей шифрование данных стало более изощренным и актуальным. Благодаря созданию новых мощных компьютеров, технологий сетевых и нейронных вычислений стало возможно «взломать» криптографические системы, до недавнего времени считавшиеся практически нераскрываемыми. Вместе с тем расширилось использование компьютерных сетей, в частности, глобальной сети Internet, по которым передаются большие объемы информации государственного, военного, коммерческого и частного характера, доступ к которой для посторонних лиц недопустим. Все это привело к тому, что очень быстро практическая криптография в деловой сфере сделала огромный скачок в развитии, причем сразу по нескольким направлениям:

- разработаны стойкие блочные шифры с секретным ключом, предназначенные для решения классической задачи — обеспечения секретности и целостности передаваемых или хранимых данных;
- созданы методы решения новых, нетрадиционных задач защиты информации, наиболее известными из которых являются задачи цифровой подписи документа и открытого распределения ключей.

Современные криптографические системы позволяют шифровать сообщения так, что на их раскрытие могут понадобиться десятки или даже сотни лет непрерывной работы.

В настоящее время используются различные компьютерные криптоалгоритмы и программы для шифрования данных, наиболее известны из них DES, RSA, PGP, ГОСТ 28147—89.

Кодирование и шифрование — основные методы криптографической защиты. Наряду с ними к криптографическим методам относят методы рассечения (разнесения) и сжатия (расширения) информации.

Рассечение (разнесение) информации заключается в том, что массив защищенных данных делится на части, каждая из которых в отдельности не позволяет раскрыть содержание защищаемой информации. Эти фрагменты можно передавать по нескольким источникам, разносить по времени и по месту записи на дискете или любом другом запоминающем устройстве.

Сжатие (расширение) информации представляет собой замену часто встречающихся одинаковых последовательностей символов некоторыми заранее выбранными символами или же подмешивание дополнительной информации.

Основные положения и определения криптографии

Очень часто через известную всем сеть Internet передается достаточно важная конфиденциальная информация. Потеря, подделка такой информации или несанкционированный доступ к ней может привести к самым серьезным последствиям. Популярный рекламный слоган «Интернет доступен всем» говорит о многом, и, к сожалению, не только о хорошем. Ясно, что доступность этого ресурса именно всем и влечет за собой определенную опасность для всех. Действительно, открытость и прозрачность устройства сети является одним из необходимых условий ее роста и распространения. Однако глобальная сеть объединяет в настоящее время людей с самыми разными интересами и наклонностями. Пользователями сети являются не только люди с кристально чистыми намерениями, но и те, кто использует информацию в корыстных целях, т. е. лица, которые хотят и, главное, могут это сделать, используя достаточно много существующих точек в сети, где информация может быть перехвачена или сфальсифицирована.

Мы живем в эпоху господства информационных технологий, когда обладание информацией является определяющей силой. И эта информация нуждается сегодня в серьезной защите.

Проблемой защиты информации путем ее преобразования занимается криптология (kryptos — тайный, logos — сообщение). Она имеет два направления: криптографию и криптоанализ. Цели этих направлений прямо противоположны.

Криптография занимается поиском, исследованием и разработкой математических методов преобразования информации, основой которых является шифрование.

Сфера интересов криптоанализа — исследование возможности расшифровки информации.

Для людей, не занимающихся вплотную проблемами информационной безопасности, криптография кажется сложным и непонятным делом, связанным с шифрами, кодами и секретными сообщениями. Действительно, ее практическая реализация требует достаточно серьезных знаний. Используя более общее определение, можно сказать, что криптография — это наука об обеспечении безопасности данных. В основе криптографической защиты информации лежит ее шифрование, проще говоря, преобразование данных к такому виду, что они становятся нечитабельными для тех, для кого не предназначены. Чтобы обеспечить нечитабельность для одних и доступность информации для других, необходимо соблюдать 4 основные правила обеспечения безопасности:

- конфиденциальность;
- аутентификацию;
- целостность;
- контроль участников взаимодействия.

С конфиденциальностью и аутентификацией все ясно: не зная ключа, сообщение прочитать весьма затруднительно. То есть, управляя раздачей ключей, вы управляете и доступом к информации.

Для контроля целостности используется построение так называемого дайджеста сообщения или электронной подписи. При построении этой подписи используется

специальная функция, схожая с известной функцией CRC (Control Cyclic Code). Результаты работы этой функции шифруются. Получателю остается только выполнить эту функцию для принятого сообщения и сравнить результат с расшифрованным.

Современная криптография изучает и развивает 4 основные направления:

- ❑ симметричные криптосистемы (с секретным ключом);
- ❑ несимметричные криптосистемы (с открытым ключом);
- ❑ системы электронной подписи;
- ❑ системы управления ключами.

Расширение практического применения криптографии в сетях, а также появление современных криптографических методов привело к необходимости введения понятий, определений и собственного математического аппарата в этой области.

Термин «криптография» далеко ушел от своего первоначального значения — «тайнопись, тайное письмо». Сегодня эта дисциплина объединяет методы защиты информационных взаимодействий совершенно различного характера, опирающихся на преобразование данных по секретным алгоритмам, включая и алгоритмы, использующие секретные параметры.

Основные направления использования криптографических методов — это передача конфиденциальной информации по каналам связи (например, электронная почта), установление подлинности передаваемых сообщений, хранение информации (документов, баз данных) на носителях в зашифрованном виде.

Современные криптографические системы обеспечивают высокую стойкость зашифрованных данных за счет поддержания режима секретности криптографического ключа. Однако на практике любой шифр, используемый в той или другой криптосистеме, поддается раскрытию с определенной трудоемкостью. В связи с этим возникает необходимость оценки **криптостойкости** применяемых шифров в алгоритмах криптопреобразования.

Обеспечение аутентичности, целостности и неоспоримости информации

Помогая сохранить содержание сообщения в тайне, криптографию можно использовать для обеспечения:

- G аутентификации;
- O целостности;
- ❑ неоспоримости.

При аутентификации получателю сообщения требуется убедиться, что оно исходит от конкретного отправителя. Злоумышленник не может прислать фальшивое сообщение от чьего-либо имени.

При определении целостности получатель сообщения в состоянии проверить, были ли внесены какие-нибудь изменения в полученное сообщение во время его передачи. Злоумышленнику не позволено заменить настоящее сообщение на фальшивое.

Неоспоримость необходима для того, чтобы отправитель сообщения не смог впоследствии отрицать, что он является автором этого сообщения.

Перечисленные задачи часто приходится решать на практике для организации обмена информацией при помощи компьютеров и компьютерных сетей. Подобные же

задачи возникают и в случае личностного человеческого общения: часто требуется проверить, а действительно ли ваш собеседник тот, за кого он себя выдает, и подлинны ли предъявленные им документы, будь то паспорт, водительское удостоверение или страховой полис. Вот почему в обыденной жизни не обойтись без аутентификации, проверки целостности и доказательства неоспоримости, а значит, и без криптографии.

Эффективность аутентификации определяется, прежде всего, отличительными особенностями каждого пользователя. В качестве таковых часто применяются пароли. Однако пользователи, как правило, стараются создавать легко запоминающиеся пароли, а значит, и легкие для их угадывания или подбора. С другой стороны, сложные пароли приходится записывать (например, на листке настольного календаря). Решение данной проблемы возможно закрытием выбранных паролей криптографическими методами. В настоящее время аутентификация, осуществляемая пользователем, обеспечивается с помощью:

- смарт-карт;
- средств биометрии;
- клавиатуры компьютера;
- криптографии с уникальными ключами для каждого пользователя.

Целостность информации обеспечивается с помощью криптографических контрольных сумм и механизмов управления доступом и привилегий. В качестве криптографической контрольной суммы для обнаружения преднамеренной или случайной модификации данных используется код аутентификации сообщения — MAC (Message Autentification Code). Принцип обнаружения модификации данных в этом случае состоит в следующем. С помощью криптографического алгоритма и секретного ключа на основании содержания файла вычитается начальное значение MAC, которое хранится в запоминающем устройстве. Если необходимо проверить целостность файла, производится повторный расчет MAC с использованием того же секретного ключа. В случае совпадения начального и повторного значений MAC принимают решение об отсутствии модификации файла.

Кроме того, для обнаружения несанкционированных изменений в передаваемых сообщениях можно применить:

- электронно-цифровую подпись (ЭЦП), основанную на криптографии с открытым и секретными ключами;
- программы обнаружения вирусов;
- назначение соответствующих прав пользователям для управления доступом;
- точное выполнение принятого механизма привилегий.

Неоспоримость получаемого сообщения подтверждается широко используемой электронно-цифровой подписью.

Использование шифров и ключей

Первичным в области криптографии является понятие кодирования информации, которое обычно трактуется в энциклопедиях, энциклопедических словарях и специальных книгах как синоним понятия «представление информации». Реализация этих понятий может представлять информацию в виде рисунков, чисел, текстов, нотных записей, последовательностей электромагнитных, оптических или других сигналов (например, телеграфный код Морзе) и т. д.

Часто под словом «кодирование» понимают также не только способ представления информации, но еще и сам процесс преобразования данных из одного представления в другое. Процесс обратного преобразования в таком случае обычно называют декодированием. Под словом «код» в самом общем его смысле понимают тот самый **конкретный** способ представления (кодирования) информации, который используется в каждом конкретном случае.

Первой и наиболее важной целью кодирования информации на протяжении всей истории человечества была и остается возможность обмена этой информацией между людьми. В частности, при фиксации информации на материальных носителях, «живущих» дольше, чем конкретный человек или поколение людей, появилась реальная возможность передачи опыта и накопленных знаний будущим поколениям в виде символов, рисунков или текстов. Можно без преувеличения сказать, что именно широкое распространение методов кодирования информации в виде печатных текстов, которое стало по-настоящему массовым после изобретения книгопечатания, и послужило базой для современной науки и промышленности. Распространение способов кодирования информации в виде печатных текстов обеспечило защиту кодируемой информации от преднамеренных или случайных искажений при ее передаче или хранении.

С появлением новых способов передачи электромагнитных сигналов, кодирование информации в виде последовательностей электромагнитных импульсов (радио, телевидение) стало настолько привычным и обыденным, что вряд ли требует каких-то дополнительных пояснений. С распространением способов кодирования и передачи информации для защиты от искажений информации, передаваемой или хранимой в виде последовательности электромагнитных импульсов, была создана новая наука — теория кодов, обнаруживающих и исправляющих ошибки.

И третья задача, возникшая одновременно с обменом информацией (сообщениями), — это сокрытие смысла передаваемой информации от посторонних. Объективно, причиной возникновения такой проблемы служат противоречия интересов отдельных людей или групп в реальной жизни, которые и порождают необходимость скрывать **какую-то** информацию.

Для сокрытия смысла передаваемых сообщений используются специальные **коды — шифры,** ключи, представляющие собой совокупность обратимых преобразований множества открытых данных на множество зашифрованных данных, осуществляемых по определенным правилам с применением ключа. Как сообщает древнегреческий историк Геродот, секретные донесения на деревянных табличках, покрытых воском, предупредили спартанских вождей о надвигающемся вторжении персов. Таким образом, шифрование применялось в военных целях уже с 479 г. до н. э.

Любой шифр, служащий для защиты информации от посторонних (то есть для сокрытия смысла передаваемого сообщения), должен допускать ее однозначное ее декодирование (расшифрование, восстановление) теми, для кого она предназначается.

Конкретный ключ выбирается случайно из огромного множества однотипных кодов, и получателю информации сообщается заранее, какой из кодов он должен применить для декодирования. Обычно тот параметр, который описывает конкретный код, стараются сделать максимально простым по виду, не имеющим каких-либо структурных закономерностей, — это просто некая строка символов или число. Его, как это повелось исторически, называют ключом или номером кода.

Если получатель информации знает ключ, он легко расшифрует закодированные данные. А вот если у него нет нужного ключа, тогда он вынужден перебирать все возможные его варианты, что при очень большом их количестве практически невозможно. Реально используют классы кодов с таким числом возможных вариантов, чтобы их перебор потребовал бы, по крайней мере, нескольких сотен или тысяч лет непрерывной работы самых мощных суперкомпьютеров.

Некоторая, весьма узкая часть класса защитных кодов, служащих для сокрытия информации от посторонних, получила название шифров. Шифры всегда были принадлежностью государственных спецслужб, которые и сейчас всеми силами стараются сохранить эту монополию, хотя и без видимого успеха.

Практически единственная возможность выделить шифры в классе всех защитных кодов — дать полное описание конкретного класса алгоритмов преобразования (кодирования) информации. Это и было сделано правительственными службами США при описании алгоритма шифрования DES, в СССР — при описании алгоритма шифрования ГОСТ 28147-89, в Японии — при описании алгоритма шифрования FEAL и т. д.

Все другие способы дать их формальное описание наталкиваются на непреодолимые логические противоречия. Так, попытка в тексте стандарта на шифрование данных в компьютерных сетях СССР ГОСТ 28147-89 (ныне принимаемого как стандарт на шифрование несекретных данных в России) дать формальное определение, что же такое шифр, привела к так называемому логическому порочному кругу определений, когда одно понятие определяется через другое, а то, в свою очередь, определяется вновь через первое.

Поэтому, строго говоря, все, что регламентирует создание, продажу или использование шифров или их реализующих устройств и программ, так называемых шифровальных средств, относится только к реализации именно того общедоступного алгоритма кодирования информации, который официально признан в данной стране шифром (мы не касаемся здесь вопросов применения секретных и сов. секретных шифров, применяемых в государственных системах засекреченной связи).

В информационных системах предприятий шифрование широко используется уже много лет. А домашние пользователи начинают приобщаться к нему только сейчас, причем иногда они об этом и не знают.

Так, браузеры Microsoft Internet Explorer и Netscape Communicator содержат встроенные средства шифрования для электронной торговли. Без каких бы то ни было указаний со стороны пользователя номера кредитных карточек передаются с компьютера пользователя на Web-сервер зашифрованными по симметричному протоколу SSL (Secure Sockets Layer). По умолчанию используются 40-битные ключи, но для обоих браузеров доступна также версия с 128-битными ключами.

Можно еще надежнее защитить данные. Популярные почтовые программы, в том числе Microsoft Outlook и Lotus Notes, в настоящее время позволяют шифровать письма. Многие «почтальоны» поддерживают протокол несимметричного шифрования S/MIME (Secure MIME — Защищенный MIME), хотя лишь немногие пользователи его применяют. Для работы с протоколом S/MIME требуется цифровой идентификатор — «сертификат», который нужно покупать у компаний, примерно за 15 долларов в год.

Дополнительную защиту могут обеспечить автономные утилиты, которые шифруют не только почтовые сообщения, но и файлы с изображениями, документы, папки на жестком диске и т. д. Наиболее популярной из них является PGP.

Аналитики предполагают, что применение систем сильного шифрования расширится благодаря недавним изменениям в регулировании экспорта криптографических систем Министерством торговли США. Еще не так давно большинство программ шифрования проходили по категории вооружений и подпадали под те же экспортные ограничения, что ручные гранаты или ракеты. Экспорт шифровальных программ с ключами длиннее 40 бит запрещался под страхом высокого штрафа или тюрьмы. Новые правила разрешают вывоз из США некоторых систем шифрования. По словам аналитиков, поначалу это не будет иметь заметного эффекта, поскольку большинство шифровальных программ созданы за пределами Штатов, а импорт программного обеспечения этого типа уже был разрешен. Выгоду от изменений в законодательстве должны получить производители программного обеспечения, которым больше не нужно будет разрабатывать криптографические средства за границей.

Главным компонентом любой системы защиты информации является ее ключ. С одной стороны, под ключом к информации следует понимать технологию шифрования/дешифрования, содержащую алгоритм и шифр, с другой — это внешний электронный идентификатор, подключаемый пользователем к стандартному компьютеру в тот момент, когда необходимо получить доступ к засекреченной информации. Какой электронный идентификатор лучше? Вероятно, тот, который не требует модернизации стандартного компьютера. Удачным примером подобного устройства служит ключ, поставляемый в комплекте SecretDisk для шины USB. Некоторые системы не предполагают использование электронного идентификатора. В этом случае при формировании личного ключа задействуют только пароль. Эмуляция такого пароля при попытке взлома может быть более простой задачей, чем подбор шифра. В любом случае предпочтительнее иметь комбинацию личного электронного идентификатора и пароля.

И в заключение надо отметить, что систем защиты информации для малых и домашних офисов не так уж много: большинству пользователей придется выбирать между программными решениями в чистом виде и аппаратно-программным комплексом SecretDisk и ему подобными.

Характеристика распространенных алгоритмов шифрования

В настоящее время наблюдается резкий рост объемов информации (в том числе и конфиденциальной), передаваемой по открытым каналам связи. По обычным телефонным каналам осуществляется взаимодействие между банками, брокерскими конторами и биржами, удаленными филиалами организаций, проводятся торги ценными бумагами. Почта любого владельца современного персонального компьютера может быть перехвачена, а коллегам ничто не мешает ознакомиться с вашими документами. Поэтому все более актуальной становится проблема защиты передаваемой информации. Несмотря на то что конкретные реализации систем защиты информации могут существенно отличаться друг от друга из-за различия методов и алгоритмов передачи данных, все они должны обеспечивать решение триединой задачи:

- конфиденциальность информации (доступность ее только для того, кому она предназначена);

- целостность информации (ее достоверность и точность, а также защищенность от преднамеренных и непреднамеренных искажений);
- готовность информации (использование в любой момент, когда в ней возникает необходимость).

Успешное решение перечисленных задач возможно как за счет использования организационно-технических мероприятий, так и с помощью криптографической защиты информации. Организационно-технические мероприятия включают в себя физическую охрану объектов конфиденциальной информации, применение специального административного персонала и целый ряд других дорогостоящих технических мер по защите важных данных.

Криптографическая защита в большинстве случаев является более эффективной и дешевой. Конфиденциальность информации при этом обеспечивается шифрованием передаваемых документов или всего трафика.

Сумеет защитить ваши данные от любопытных глаз только шифрование — кодирование информации, после которого ее нельзя прочесть без специального ключа. Когда-то к шифрованию прибегали одни шпионы, но сейчас оно быстро становится мерой разумной предосторожности для всех тех, кто дома или на работе использует компьютер: это лучшее средство сохранить служебную и личную тайну.

Независимо от того, применяется автономная утилита или встроенная функция почтовой программы, процесс шифрования происходит одинаково: данные обрабатываются по определенному алгоритму, в результате чего образуется зашифрованный текст. Алгоритму для работы необходимо получить от вас одну переменную — ваш ключ.

Процесс криптографического закрытия данных может осуществляться как программно, так и аппаратно. Аппаратная реализация отличается существенно большей стоимостью, однако ей присущи и преимущества: высокая производительность, простота, защищенность и т. д. Программная реализация более практична, допускает известную гибкость в использовании. Для современных криптографических систем защиты информации сформулированы следующие требования:

- зашифрованное сообщение должно поддаваться чтению только при наличии ключа;
- число операций, необходимых для определения использованного ключа шифрования по фрагменту шифрованного сообщения и соответствующего ему открытого текста, должно быть не меньше общего числа возможных ключей;
- число операций, необходимых для расшифровывания информации путем перебора всевозможных ключей, должно иметь строгую нижнюю оценку и выходить за пределы возможностей современных компьютеров (с учетом возможности использования сетевых вычислений);
- знание алгоритма шифрования не должно влиять на надежность защиты;
- незначительное изменение ключа должно приводить к существенному изменению вида зашифрованного сообщения даже при использовании одного и того же ключа;
- структурные элементы алгоритма шифрования должны быть неизменными;
- дополнительные биты, вводимые в сообщение в процессе шифрования, должны быть полностью и надежно скрыты в шифрованном тексте;
- длина шифрованного текста должна быть равной длине исходного текста;

- не должно быть простых и легко устанавливаемых зависимостей между ключами, последовательно используемыми в процессе шифрования;
- любой ключ из множества возможных должен обеспечивать надежную защиту информации;
- алгоритм должен допускать как программную, так и аппаратную реализацию, при этом изменение длины ключа не должно вести к качественному ухудшению алгоритма шифрования.

Сам по себе криптографический алгоритм, называемый алгоритмом шифрования, представляет собой некоторую математическую функцию, используемую для шифрования и расшифровки. Точнее таких функций две: одна применяется для шифрования, а другая — для расшифрования.

Различается шифрование двух типов:

- симметричное (с секретным ключом);
- несимметричное (с открытым ключом).

При симметричном шифровании (рис. 4.2) создается ключ, файл совместно с этим ключом пропускается через программу шифрования и полученный результат пересылается адресату, а сам ключ передается адресату отдельно, используя другой (защищенный или очень надежный) канал связи. Адресат, запустив ту же самую шифровальную программу с полученным ключом, сможет прочитать сообщение. Симметричное шифрование не так надежно, как несимметричное, поскольку ключ может быть перехвачен, но из-за высокой скорости обмена информацией оно широко используется, например, в операциях электронной торговли.

Несимметричное шифрование сложнее, но и надежнее. Для его реализации (рис. 4.3) нужны два взаимосвязанных ключа: открытый и закрытый. Получатель сообщает всем желающим свой открытый ключ, позволяющий шифровать для него сообщения. Закрытый ключ известен только получателю сообщения. Когда кому-то нужно послать зашифрованное сообщение, он выполняет шифрование, используя открытый ключ получателя. Получив сообщение, последний расшифровывает его с помощью своего закрытого ключа. За повышенную надежность несимметричного шифрования приходится платить: поскольку вычисления в этом случае сложнее, то процедура расшифровки отнимает больше времени.

Когда надежность криптографического алгоритма обеспечивается за счет сохранения в тайне сути самого алгоритма, такой алгоритм шифрования называется ограниченным. Ограниченные алгоритмы представляют значительный интерес с точки зрения истории криптографии, однако совершенно непригодны при современных

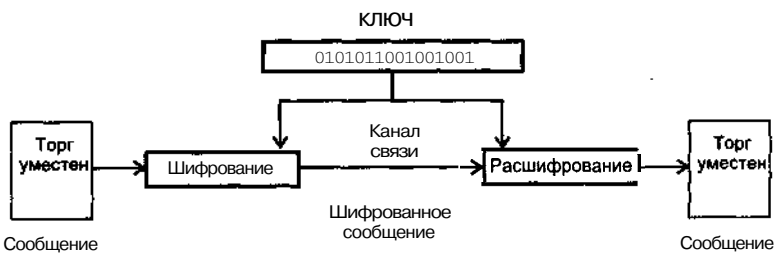


Рис. 4.2. Симметричное шифрование

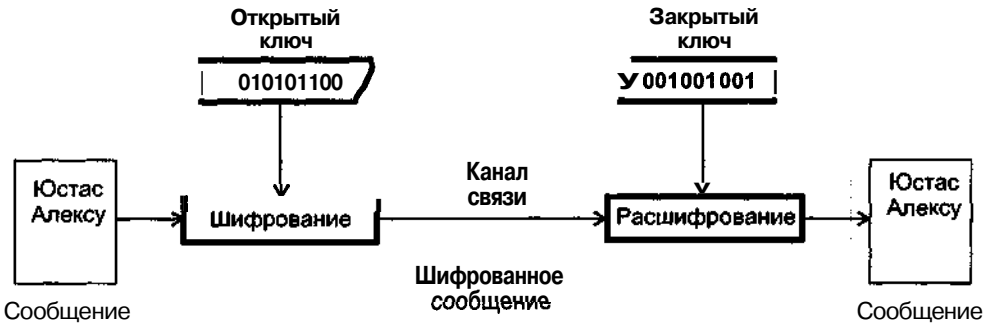


Рис. 4.3. Несимметричное шифрование

требованиях, предъявляемых к шифрованию. Ведь в этом случае каждая группа пользователей, желающих обмениваться секретными сообщениями, должна обзавестись своим оригинальным алгоритмом шифрования. Использование готового оборудования и стандартных программ исключено, поскольку приведет к тому, что любой сможет приобрести это оборудование и эти программы и ознакомиться с заложенным в них алгоритмом шифрования. Тогда придется разрабатывать собственный криптографический алгоритм, причем делать это надо будет каждый раз, когда кто-то из пользователей группы захочет ее покинуть или когда детали алгоритма станут случайно известны посторонним.

В современной криптографии указанные выше проблемы решаются с помощью использования ключа, который нужно выбирать среди значений, принадлежащих множеству, называемому ключевым пространством. Функции шифрования и расшифровки зависят от этого ключа. Некоторые алгоритмы шифрования используют различные ключи для шифрования и расшифрования. Это означает, что ключ шифрования отличается от ключа расшифрования.

Надежность алгоритма шифрования с использованием ключей достигается за счет их надлежащего выбора и последующего хранения в строжайшем секрете. Это означает, что такой алгоритм не требуется держать в тайне. Можно организовать массовое производство криптографических средств, в основу функционирования которых положен данный алгоритм. Даже зная криптографический алгоритм, злоумышленник все равно не сможет прочесть зашифрованные сообщения, поскольку он не знает секретный ключ, использованный для их зашифрования.

Как уже говорилось, существуют две разновидности алгоритмов шифрования с использованием ключей — симметричные (одноключевые) и несимметричные (двухключевые). В большинстве симметричных алгоритмов применяют всего Один ключ. Такие алгоритмы именуются одноключевыми, или алгоритмами с секретным ключом, и требуют, чтобы отправитель сообщений и их получатель заранее условились о том, каким ключом они будут пользоваться. Надежность одноключевого алгоритма определяется выбором ключа, поскольку его знание дает возможность злоумышленнику без помех расшифровывать все перехваченные сообщения. Поэтому выбранный ключ следует хранить в тайне от посторонних.

Симметричные алгоритмы шифрования подразделяются на:

- потоковые (поточные);
- блочные.

Алгоритмы, в которых открытый текст обрабатывается побитно, называются потоковыми алгоритмами или потоковыми шифрами. В других алгоритмах открытый текст разбивается на блоки, состоящие из нескольких бит. Такие алгоритмы называются блочными, или блочными шифрами. В современных компьютерных алгоритмах блочного шифрования длина блока обычно составляет 64 бита.

Основное преимущество несимметричных алгоритмов перед симметричными состоит в том, что секретный ключ, позволяющий расшифровывать всю получаемую информацию, известен только получателю сообщения. Кроме того, первоначальное распределение ключей в системе не требует передачи секретного ключа, который может быть перехвачен нарушителем. Несимметричные алгоритмы получили новое качество — на их основе строятся протоколы цифровой подписи. Для аутентификации с использованием симметричных алгоритмов часто требуется участие доверенной третьей стороны, которая, как, например, в схеме Kerberos, хранит копии секретных ключей всех пользователей. Компрометация третьей стороны может привести к компрометации всей системы аутентификации. В системах с открытым ключом эта проблема устранена потому, что каждый пользователь отвечает за безопасность только своего секретного ключа.

Симметричные алгоритмы при обнаружении в них каких-либо слабостей могут быть доработаны путем внесения небольших изменений, а для несимметричных такая возможность отсутствует.

Симметричные алгоритмы работают значительно быстрее, чем алгоритмы с открытым ключом. На практике несимметричные алгоритмы шифрования часто применяются в совокупности с симметричными алгоритмами: открытый текст зашифровывается симметричным алгоритмом, а секретный ключ этого симметричного алгоритма зашифровывается на открытом ключе несимметричного алгоритма. Такой механизм называют цифровым конвертом (digital envelope).

Наиболее широко в настоящее время применяются следующие алгоритмы шифрования:

- DES (Data Encryption Standard);
- Blowfish;
- IDEA (International Decryption-Encryption Algorithm);
- ГОСТ 28147-89;
- RSA (авторы: Rivest, Shamir и Alderman);
- PGP.

В симметричных криптоалгоритмах (DES, ГОСТ, Blowfish, RC5, IDEA) для шифрования и расшифрования информации используется один и тот же секретный ключ. Достоинствами таких алгоритмов являются:

- простота программной и аппаратной реализации;
- высокая скорость работы в прямом и обратном направлениях;
- обеспечение необходимого уровня защиты информации при использовании коротких ключей.

К основным недостаткам этих криптоалгоритмов следует отнести увеличение затрат по обеспечению дополнительных мер секретности при распространении ключей, а

также то, что алгоритм с секретным ключом выполняет свою задачу только в условиях полного доверия корреспондентов друг другу.

В несимметричных криптоалгоритмах (RSA, PGP, ECC) прямое и обратное преобразования выполняются с использованием открытого и секретного ключей, которые не имеют взаимосвязи, позволяющей по одному ключу вычислить другой. С помощью открытого ключа практически любой пользователь может зашифровать свое сообщение или проверить электронно-цифровую подпись. Расшифровать такое сообщение или поставить подпись может только владелец секретного ключа.

Такие алгоритмы позволяют реализовать протоколы типа цифровой подписи, обеспечивают открытое распространение ключей и надежную аутентификацию в сети, устойчивую даже к полному перехвату трафика.

Шифрование в компьютерной сети

Поскольку высок уровень компьютерных преступлений, связанных с несанкционированным доступом к информации в сетях различного масштаба, существует необходимость создавать определенные механизмы защиты сетей. Практика показала, что единственно надежным механизмом защиты информации в сетевых каналах связи является ее шифрование, а значит, использование криптографического преобразования конфиденциальных данных. При этом обеспечение защиты информации указанным методом не должно нарушать работу сети в реальном масштабе времени, что возможно при выполнении шифрования со скоростью до 1 Гбит/с и выше.

Рассмотрим особенности шифрования в компьютерных сетях более подробно.

Виды шифрования в сетевых каналах связи

Одной из отличительных характеристик любой компьютерной сети является ее деление на так называемые уровни, каждый из которых отвечает за соблюдение определенных условий и выполнение функций, необходимых для общения между компьютерами, связанными в сеть. Это деление на уровни имеет фундаментальное значение для создания стандартных компьютерных сетей. Поэтому в 1984 году несколько международных организаций и комитетов объединили свои усилия и выработали примерную модель компьютерной сети, известную под названием OSI (Open Systems Interconnection — Модель открытых сетевых соединений).

Согласно модели OSI, коммуникационные функции разнесены по уровням. Функции каждого уровня не зависят от функций ниже- и вышележащих уровней. Каждый уровень может непосредственно общаться только с двумя соседними. Модель OSI определяет 7 уровней: верхние 3 служат для связи с конечным пользователем, а 4 нижних ориентированы на выполнение коммуникационных функций в реальном масштабе времени (рис. 4.4).

Теоретически шифрование данных для передачи по каналам связи компьютерной сети может осуществляться на любом уровне модели OSI. На практике это обычно делается либо на самых нижних, либо на самых верхних уровнях. Если данные шифруются на нижних уровнях, шифрование называется канальным, а если на верхних, то такое шиф-

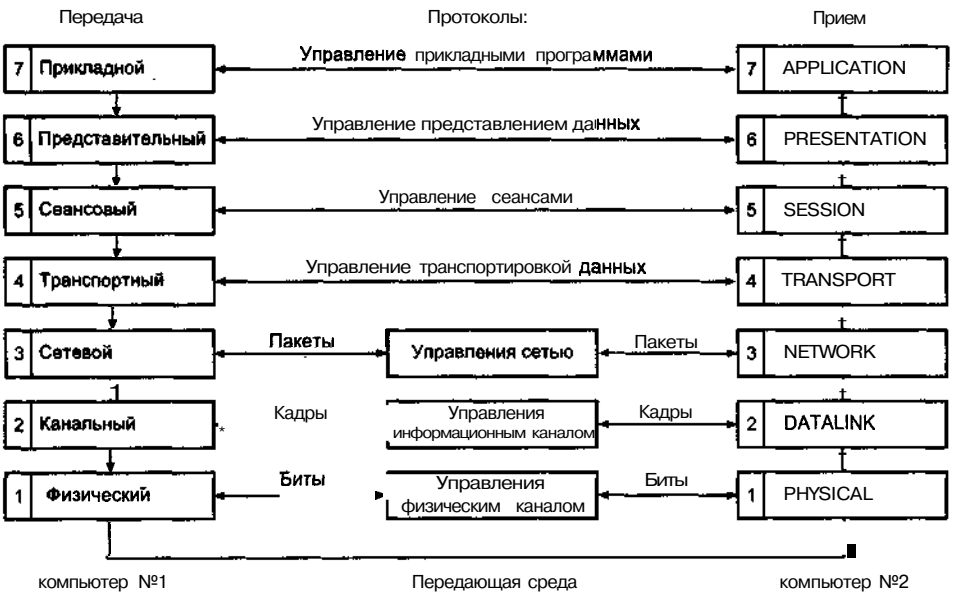


Рис. 4.4. Модель открытых сетевых соединений

рование называется сквозным. Оба этих подхода к шифрованию данных имеют свои преимущества и недостатки. Возможна комбинация указанных видов шифрования (рис. 4.5).

При канальном шифровании шифруются абсолютно все данные, проходящие по каждому каналу связи, включая открытый текст сообщения, а также информацию о его маршрутизации и об используемом коммуникационном протоколе. Однако в этом случае любой интеллектуальный сетевой узел (например, коммутатор) будет вынужден расшифровывать входящий поток данных, чтобы соответствующим образом его обработать, снова зашифровать и передать на другой узел сети.

Тем неменее, канальное шифрование представляет собой очень эффективное средство защиты информации в компьютерных сетях. Поскольку шифрованию подлежат все данные, передаваемые от одного узла сети к другому, у криптоаналитика нет никакой дополнительной информации о том, кто служит источником этих данных, кому они предназначены, какова их структура и т. д. А если еще позаботиться и о том, чтобы, пока канал простаивает, передавать по нему случайную битовую последовательность, сторонний наблюдатель не сможет даже сказать, где начинается и где заканчивается текст передаваемого сообщения.

Не слишком сложной является и работа с ключами. Одинаковыми ключами следует снабдить только два соседних узла сети связи, которые затем могут менять используемые ключи независимо от других пар узлов.

Самый большой недостаток канального шифрования заключается в том, что данные приходится шифровать при передаче по каждому физическому каналу компьютерной сети. Отправка информации в незашифрованном виде по какому-то из каналов ставит под угрозу обеспечение безопасности всей сети. В результате стоимость реализации канального шифрования в больших сетях может оказаться чрезмерно высокой.

Рис. 4.5. Виды шифрования в компьютерной сети

Кроме того, при использовании канального шифрования дополнительно потребуется защищать каждый узел компьютерной сети, по которому передаются данные. Если абоненты сети полностью доверяют друг другу, и каждый ее узел находится там, где он защищен от злоумышленников, на этот недостаток канального шифрования можно не обращать внимания. Однако на практике такое положение встречается чрезвычайно редко. Ведь в каждой фирме есть конфиденциальные данные, ознакомиться с которыми могут только сотрудники одного отдела, а за его пределами доступ к этим данным необходимо ограничивать до минимума.

При сквозном шифровании криптографический алгоритм реализуется на одном из верхних уровней модели OSI. Шифрованию подлежит только содержательная часть сообщения. По мере шифрования добавляется служебная информация, необходимая для маршрутизации сообщения, и результат переправляется на более низкие уровни для отправки адресату.

Передаваемое сообщение теперь не требуется постоянно шифровать и расшифровывать при его прохождении через каждый промежуточный узел сети. Оно остается зашифрованным на всем пути от отправителя к получателю.

Основная проблема, с которой сталкиваются пользователи сетей, где применяется сквозное шифрование, связана с тем, что служебная информация, используемая для маршрутизации сообщений, передается по сети в незашифрованном виде. Опытный криптоаналитик может извлечь для себя массу полезной информации, зная, кто с кем, как долго и в какие часы общается через компьютерную сеть. Для этого ему даже не потребуется быть в курсе предмета общения.

Сквозное шифрование по сравнению с канальным характеризуется более сложной работой с ключами, так как каждая пара пользователей компьютерной сети должна быть снабжена одинаковыми ключами, прежде чем они смогут связаться друг с другом. А поскольку криптографический алгоритм реализуется на верхних уровнях модели OSI, приходится также сталкиваться со многими существенными различиями в коммуникационных протоколах и интерфейсах в зависимости от типов сетей и объединяемых в сеть компьютеров. Все это затрудняет практическое применение сквозного шифрования.

Комбинация канального и сквозного шифрования данных в компьютерной сети обходится значительно дороже, чем каждое из них. Однако именно такой подход позволяет наилучшим образом защитить данные, передаваемые по сети. Шифрование в каждом канале связи не позволяет противнику анализировать служебную информацию, используемую для маршрутизации, а при сквозном шифровании уменьшается вероятность доступа к незашифрованным данным в узлах сети.

При комбинированном шифровании работа с ключами ведется следующим образом: сетевые администраторы отвечают за ключи, используемые при канальном шифровании, а о ключах, применяемых при сквозном шифровании, заботятся сами пользователи.

Аппаратное шифрование

Большинство средств криптографической защиты данных реализовано в виде специализированных физических устройств. Эти устройства встраиваются в линию связи и шифруют всю передаваемую по ней информацию. Преобладание аппаратного шифрования над программным обусловлено несколькими причинами:

- более высокая скорость шифрования;
- О аппаратуру легче физически защитить от проникновения извне;
- аппаратура шифрования более проста в отладке.

Криптографические алгоритмы состоят из огромного числа сложных операций с битами открытого текста. Современные универсальные компьютеры плохо приспособлены для эффективного выполнения этих операций, а специализированное оборудование умеет делать это гораздо быстрее.

Программа, выполняемая на персональном компьютере, практически беззащитна. Вооружившись отладчиком, злоумышленник может внести в нее скрытые изменения, чтобы понизить стойкость используемого криптографического алгоритма, и никто ничего не заметит. Аппаратура же обычно помещается в особые контейнеры, чтобы нельзя было изменить схему ее функционирования. Чип покрывают специальным химическим составом, и при любой попытке преодолеть защитный слой этого чипа происходит самоуничтожение его внутренней логической структуры. И даже в случае, когда электромагнитное излучение может служить хорошим источником информации о том, что творится внутри микросхемы, от этого излучения легко избавиться, заэкранировав микросхему. Аналогичным образом можно заэкранировать и компьютер, однако сделать это гораздо сложнее, чем миниатюрную микросхему.

Очень часто шифрование требуется там, где дополнительное компьютерное оборудование совершенно излишне. Телефоны, факсимильные аппараты и модемы значительно дешевле оборудовать устройствами аппаратного шифрования, чем встраивать в них микрокомпьютеры с соответствующим программным обеспечением.

Даже в компьютерах установка специализированного шифровального оборудования создает меньше проблем, чем модернизация системного программного обеспечения с целью добавления в него функций шифрования данных. В идеале шифрование должно осуществляться незаметно для пользователя. Чтобы добиться этого при помощи программных средств, средства шифрования должны быть упрятаны глубоко в недра операционной системы. С готовой и отлаженной операционной системой проделать это безболезненно не так-то просто. Но даже любой непрофессионал сможет подсоединить шифровальный блок к персональному компьютеру, с одной стороны, и к внешнему модему, с другой.

Современный рынок аппаратных средств шифрования информации предлагает потенциальным покупателям следующие разновидности таких средств:

- самодостаточные шифровальные модули (они самостоятельно выполняют всю работу с ключами);
- блоки шифрования в каналах связи;
- шифровальные платы расширения.

Большинство устройств первого и второго типов являются узкоспециализированными, и поэтому прежде чем принимать окончательное решение об их приобретении,

необходимо досконально изучить ограничения, которые при установке накладывают эти устройства на общую конструкцию, операционные системы и прикладное программное обеспечение. А иначе можно выбросить деньги на ветер, ни на йоту не приблизившись к желанной цели. Правда, иногда выбор облегчается тем, что некоторые компании торгуют коммуникационным оборудованием, которое уже имеет предустановленную аппаратуру шифрования данных.

Платы расширения для персональных компьютеров являются более универсальным средством аппаратного шифрования и обычно могут быть легко сконфигурированы таким образом, чтобы шифровать всю информацию, которая записывается на жесткий диск компьютера, а также все данные, пересылаемые на дискеты и в последовательные порты. Как правило, защита от электромагнитного излучения в шифровальных платах расширения отсутствует, поскольку нет смысла защищать эти платы, если аналогичные меры не предпринимаются в отношении всего компьютера.

Программное шифрование файлов

Любой криптографический алгоритм можно реализовать в виде соответствующей программы. Преимущества такой реализации очевидны: программные средства шифрования легко копировать, они просты в использовании, их нетрудно модифицировать в соответствии с конкретными потребностями.

Во всех распространенных операционных системах имеются встроенные средства шифрования файлов. Обычно они предназначены для шифрования отдельных файлов, и работа с ключами целиком возлагается на пользователя. Поэтому применение этих средств требует особого внимания. Во-первых, ни в коем случае нельзя хранить ключи на диске вместе с зашифрованными с их помощью файлами, а, во-вторых, незашифрованные копии файлов необходимо удалить сразу после шифрования.

Конечно, злоумышленник может добраться до компьютера и незаметно внести нежелательные изменения в программу шифрования. Однако основная проблема состоит совсем не в этом. Если злоумышленник в состоянии проникнуть в помещение, где установлен компьютер, он вряд ли будет возиться с программой, а просто установит скрытую камеру в стене, подслушивающее устройство в телефон или датчик для ретрансляции электромагнитного излучения в компьютер. В конце концов, если злоумышленник может беспрепятственно все это сделать, сражение с ним проиграно, даже еще не начавшись.

На первый взгляд, шифрование файлов можно полностью уподобить шифрованию сообщений, отправителем и получателем которых является одно и то же лицо, а средой передачи служит одно из компьютерных устройств хранения данных (магнитный или оптический диск, магнитная лента, оперативная память). Однако все не так просто, как кажется на первый взгляд.

Если при передаче по коммуникационным каналам сообщение затеряется по пути от отправителя к получателю, его можно попытаться передать снова. При шифровании данных, предназначенных для хранения в виде компьютерных файлов, дела обстоят иначе. Если вы не в состоянии расшифровать свой файл, вам вряд ли удастся сделать это и со второй, и с третьей, и даже с сотой попытки. Ваши данные будут потеряны раз и навсегда. Это означает, что при шифровании файлов необходимо предусмотреть специальные механизмы предотвращения возникновения ошибок в шифротексте.

Криптография помогает превратить большие секреты в маленькие. Вместо того чтобы безуспешно пытаться запомнить содержимое огромного файла, человеку достаточно его зашифровать и сохранить в памяти использованный для этой цели ключ. Если ключ применяется для шифрования сообщения, то его требуется иметь под рукой лишь до тех пор, пока сообщение не дойдет до своего адресата и не будет им успешно расшифровано. В отличие от шифрованных сообщений, шифрованные файлы могут храниться годами, и в течение всего этого времени необходимо помнить и держать в секрете соответствующий ключ.

Есть и другие особенности шифрования файлов, о которых необходимо помнить вне зависимости от применяемого криптографического алгоритма:

- нередко после шифрования файла его незашифрованная копия остается на другом магнитном диске, на другом компьютере или в виде распечатки, сделанной на принтере;
- размер блока в блочном алгоритме шифрования может значительно превышать размер отдельной порции данных в структурированном файле, в результате чего зашифрованный файл окажется намного длиннее исходного;
- скорость шифрования файлов при помощи выбранного для этой цели криптографического алгоритма должна соответствовать скоростям, на которых работают устройства ввода/вывода современных компьютеров;
- работа с ключами является довольно непростым делом, поскольку разные пользователи должны иметь доступ не только к различным файлам, но и к отдельным частям одного и того же файла.

Если файл представляет собой единое целое (например, содержит какой-то текст), восстановление этого файла в исходный вид не потребует больших усилий: перед использованием достаточно просто расшифровать весь файл. Однако если файл структурирован (например, разделен на записи и поля, как это делается в базах данных), то расшифрование всего файла целиком требуется каждый раз, когда необходим доступ к отдельным порциям данных, за счет чего работа с таким файлом чрезвычайно неэффективна. Шифрование порций данных в структурированном файле делает его уязвимым по отношению к атаке, при которой злоумышленник отыскивает в этом файле нужную порцию данных и заменяет ее на другую по своему усмотрению.

У пользователя, который хочет зашифровать каждый файл, размещенный на жестком диске компьютера, имеются две возможности. Если он использует один и тот же ключ для шифрования всех файлов, то впоследствии окажется не в состоянии разграничить доступ к ним со стороны других пользователей. Кроме того, это приведет к тому, что у криптоаналитика будет много шифротекста, полученного на одном ключе, что существенно облегчит вскрытие этого ключа.

Лучше шифровать каждый файл на отдельном ключе, а затем зашифровать все ключи при помощи мастер-ключа. Тем самым пользователи будут избавлены от суеты, связанной с организацией надежного хранения множества ключей. Разграничение доступа групп пользователей к различным файлам будет осуществляться путем деления множества всех ключей на подмножества и шифрования этих подмножеств на различных мастер-ключах. Стойкость такой криптосистемы будет значительно выше, чем в случае использования единого ключа для шифрования всех файлов на жестком диске, поскольку ключи можно генерировать случайным образом, поэтому они будут более стойкими против словарной атаки.

Общая характеристика современных стандартов шифрования

Очевидно, что в основе защиты информации лежит процесс шифрования. Лучшие умы человечества на протяжении всей истории занимались проблемами составления шифров. Главное, к чему все стремились, — это создать криптоустойчивые шифры. Разработанные шифры и соответствующие ключи в дальнейшем использовали в алгоритмах шифрования. Алгоритмов шифрования существует великое множество, мы рассмотрим лишь самые популярные из них, получившие статус стандартов. Это DES (Data Encryption Standard), RSA (алгоритм Rivest-Shamir-Adleman), PGP, наш отечественный ГОСТ 28147-89 (который в иностранной литературе чаще называется просто GOST) и другие. Причем современные шифры — это не только собственно алгоритмы шифрования, а криптографические системы, где определены также возможные типы и параметры ключей, способы организации работы с ключами и зашифрованными сообщениями, правила определения подлинности и целостности сообщений и т. п. Основа каждого стандарта — определенные математические построения, знать которые не обязательно. Гораздо важнее знать особенности и область применения того или иного стандарта.

В основе любой криптографической системы лежат алгоритм шифрования, протокол взаимодействия участвующих сторон и процедура управления ключами.

Протокол — это последовательность шагов, которые предпринимают стороны для совместного решения задачи. Все шаги следуют в порядке строгой очередности, и ни один из них не может быть сделан прежде, чем закончится предыдущий. Кроме того, любой протокол подразумевает участие, по крайней мере, двух сторон. В одиночку можно, например, смешать и выпить коктейль, но к протоколу это не имеет никакого отношения. Поэтому придется угостить кого-нибудь сделанным коктейлем, чтобы его приготовление и дегустация стали настоящим протоколом. И наконец, протокол обязательно предназначен для достижения какой-то цели.

Протоколы имеют и другие отличительные черты:

- каждый участник протокола должен быть заранее оповещен о шагах, которые ему предстоит предпринять;
- все участники протокола должны следовать его правилам добровольно, без принуждения;
- необходимо, чтобы протокол допускал только однозначное толкование, а его шаги были совершенно четко определены и не допускали возможности их неправильного понимания;
- протокол должен содержать описание реакции его участников на любые ситуации, возникающие в ходе реализации этого протокола, иными словами, недопустимым является положение, когда для возникшей ситуации протоколом не определено соответствующее действие.

Криптографическим протоколом называется такой, в основе которого лежит набор правил и процедур, определяющих использование криптоалгоритма и ключей шифрования. Однако целью криптографического протокола зачастую является не только сохранение информации в тайне от посторонних. Участники криптографического протокола могут быть близкими друзьями, у которых нет друг от друга секретов, а могут

являться настолько непримиримыми врагами, что каждый из них отказывается сообщить другому, какое сегодня число. Тем не менее, им может понадобиться поставить подписи под совместным договором или удостоверить свою личность. В данном случае нужна криптография, чтобы предотвратить или обнаружить подслушивание посторонними лицами, не являющимися участниками протокола, а также не допустить мошенничества. Поэтому часто требуется, чтобы криптографический протокол обеспечивал следующее: его участники могут сделать или узнать больше того, что определено протоколом.

В повседневной жизни нам приходится сталкиваться с протоколами буквально на каждом шагу: играя в любые игры, делая покупки в магазине или голосуя на выборах. Многими протоколами нас научили пользоваться родители, школьные учителя и друзья. Остальные мы сумели узнать самостоятельно.

Теперь люди все чаще общаются при помощи компьютеров. Компьютеры же, в отличие от большинства людей, в школу не ходили, у них не было родителей, да и учиться самостоятельно они не в стоянии. Поэтому компьютеры приходится снабжать формализованными протоколами, чтобы они смогли делать то, что люди выполняют особо не задумываясь. Например, если в магазине не окажется кассового аппарата, вы все равно сможете купить в нем необходимую вещь. Однако такое кардинальное изменение протокола поставило бы бедный компьютер в полный тупик.

Большинство протоколов, которые люди используют при общении друг с другом с глазу на глаз, хорошо себя зарекомендовали только потому, что участники имеют возможность вступить в непосредственный контакт. Взаимодействие с другими людьми через компьютерную сеть, наоборот, подразумевает анонимность. Будете ли вы играть с незнакомцем в преферанс, видя, как он тасует колоду и раздает карты? Доверите ли вы свои деньги совершенно постороннему человеку, чтобы он купил вам что-нибудь в магазине? Пошлете ли вы свой бюллетень голосования по почте, зная, что с ним сможет ознакомиться любой из почтовых работников и потом рассказать всем о ваших нетрадиционных политических пристрастиях?

Глупо считать, что компьютерные пользователи ведут себя более честно. То же самое касается и сетевых администраторов, и проектировщиков компьютерных сетей. Большинство из них и в самом деле честные люди, однако есть и такие, кто может причинить большие неприятности. Поэтому так нужны криптографические протоколы, использование которых позволяет защититься от непорядочных людей.

Остановимся на рассмотрении характеристик стандартов шифрования, наиболее часто используемых в компьютерных системах.

Популярный алгоритм шифрования данных DES применяется правительством США как стандарт с 1977 года. Для шифрования алгоритм использует 64-битный ключ, блок данных из 64-и бит и 16-и проходов (циклов). Этот алгоритм достаточно быстр и эффективен. Однако в изначальном виде этот стандарт недостаточно криптоустойчив, т. к. прямые атаки с перебором ключей занимают, при сегодняшнем уровне технологий, разумный срок. Поэтому в настоящее время используются всевозможные его модификации, такие как 3-DES и каскадный 3-DES.

За счет внесения дополнительных изменений в алгоритм (таких, например, как введение дополнительных избыточных ключей или обратной связи) эти модификации стали гораздо более устойчивы к прямым атакам. Главным же недостатком этой системы

является то, что она использует так называемые симметричные ключи: для шифрования и дешифрации сообщения используется один и тот же секретный ключ. Поэтому необходимым условием успешного использования этой системы является наличие секретного защищенного канала для передачи ключа. Если злоумышленник перехватит ключ для шифрования, то он легко может при помощи этого же ключа осуществить расшифровку секретного сообщения. Если же защищенный канал передачи существует, то вполне разумно тогда передать и само сообщение по этому же каналу, не прибегая к процедуре шифрования.

Государственный стандарт ГОСТ 28147-89 был утвержден в 1989 году как средство обеспечения безопасности, являющееся стандартом для государственных учреждений. Хотя он и не является основным криптосредством защищенных линий правительственной связи, однако это единственный более-менее открытый стандарт такого рода для исследования и использования самым широким кругом людей. Несмотря на то что в России ГОСТ играл ту же роль, что и DES в США, этот стандарт стал употребляться и в других странах. Например, алгоритм шифрования популярного архиватора ARJ построен как раз на использовании алгоритмов ГОСТ.

ГОСТ очень схож с DES. В нем так же используются 64-битные блоки. Тем не менее есть и ряд различий, например, в ГОСТ совершается 32 прохода вместо 16-и, ключ гораздо длиннее и состоит из 256 бит и т. д. В общем, среди специалистов принято считать, что он по своим характеристикам превосходит DES. Однако в настоящее время и его расшифровка лежит в пределах современных технологий. И точно так же ему присущи все недостатки алгоритмов, использующих симметричные ключи.

Сегодня популярен стандарт шифрования RSA. Во многом это произошло благодаря распространенности в Internet программы PGP (Pretty Good Privacy) Филиппа Зиммермана. RSA -это алгоритм несимметричного шифрования, стойкость которого зависит от сложности факторизации больших целых чисел. В настоящее время алгоритм взлома RSA не разработан математически, а за счет использования очень длинных ключей и некоторой медленности всего алгоритма перебор за разумное время попросту невозможен.

В несимметричных алгоритмах используются два разных ключа: один известен всем, а другой держится в тайне. Обычно для шифрования и расшифровки используются оба ключа. Но данные, зашифрованные одним ключом, можно расшифровать только с помощью другого ключа. Это обстоятельство делает RSA очень удобным для использования в электронной переписке. Открытый ключ делается общедоступным (его попросту можно вставлять в реквизиты вашего письма). Каждый может зашифровать сообщение и послать его вам. А расшифровать сообщение, даже зная открытый ключ, невозможно. Для этого надо знать второй, закрытый ключ, который есть только у отправителя. Однако и здесь существуют свои трудности:

- О в случае утраты секретного ключа придется уведомлять всех владельцев открытой половины о смене ключей;
- ❑ трудно убедиться в подлинности присланного вам открытого ключа.

Кроме того, отправителя легко подделать. Для того чтобы убедиться в подлинности ключа, порой используют целую «цепочку доверия», где каждый последующий передающий на 100% уверен в подлинности ключа (вследствие давнего знакомства, бли-

зости расположения к отправителю или в силу других причин), подтверждает эту подлинность своей подписью и пересылает ключ дальше.

Однако следует разделять собственно алгоритм RSA и другие продукты лаборатории RSA Data Security. Например, существует еще алгоритм RC5 — быстрый блочный шифр, который имеет размер блока 32, 64 или 128 бит, ключ длиной от 0 до 2048 бит, от 0 до 255 проходов.

Рассмотрим стандарты и системы шифрования более подробно.

Стандарт шифрования данных DES и его практическая реализация

Стандарт шифрования данных DES (Data Encryption Standard) является одним из известных алгоритмов криптографической защиты данных, используемых до недавнего времени в США. Этот стандарт — типичный представитель криптоалгоритмов, использующих симметричное шифрование. Благодаря таким качествам, как обеспечение высокого уровня защиты информации, простота и экономичность в реализации, он нашел широкое применение в различных областях государственной и военной деятельности. Рассмотрим детально принцип шифрования данных с помощью алгоритма DES.

Сегодня стандарт шифрования DES используется в Соединенных Штатах, за небольшим исключением, практически везде. Правительственная связь, электронные банковские переводы, гражданские спутниковые коммуникации и даже пароли компьютерных систем — везде, в той или иной мере, применяется защита, основанная на DES. Криптоалгоритм DES, получивший официальный статус стандарта в 1977 году, ознаменовал наступление новой эпохи в криптографии. Сертифицировав алгоритм защиты, американское правительство дало зеленую улицу изучению криптографических алгоритмов и «благословило» попытки взлома систем, построенных на их основе.

Логическая структура функционирования алгоритма DES иллюстрируется схемой обработки данных, изображенной на рис. 4.6.

Приведенная схема описывает как процесс шифрования, так и расшифровки информации. Алгоритм шифрования данных преобразует открытый текст в шифротекст или наоборот, в зависимости от режима использования. Как видно из структурной схемы, алгоритм имеет два входа по 64 бита каждый: один — для шифруемого открытого текста (при дешифровке — для шифротекста), другой — для ключа, и один 64-битный выход для полученного шифротекста (при расшифровке — для открытого текста). Из 64-х бит ключа непосредственно в процессе шифрования участвуют только 56 бит. Это связано с тем, что ключ представляется в виде восьмибитовых символов кода ASCII, каждый символ которого имеет один бит проверки на четность. Именно эти проверочные биты и не используются в алгоритме DES.

Основными блоками преобразования данных согласно алгоритму DES являются блоки перестановки, замены и сложения по модулю 2. В стандарте DES предусмотрено использование трех типов перестановок: простые, расширенные и сокращенные. Простые перестановки осуществляют изменение порядка следования бит данных. В расширенных перестановках некоторые биты используются повторно, а в сокращенных — часть битов данных просто отбрасывается.

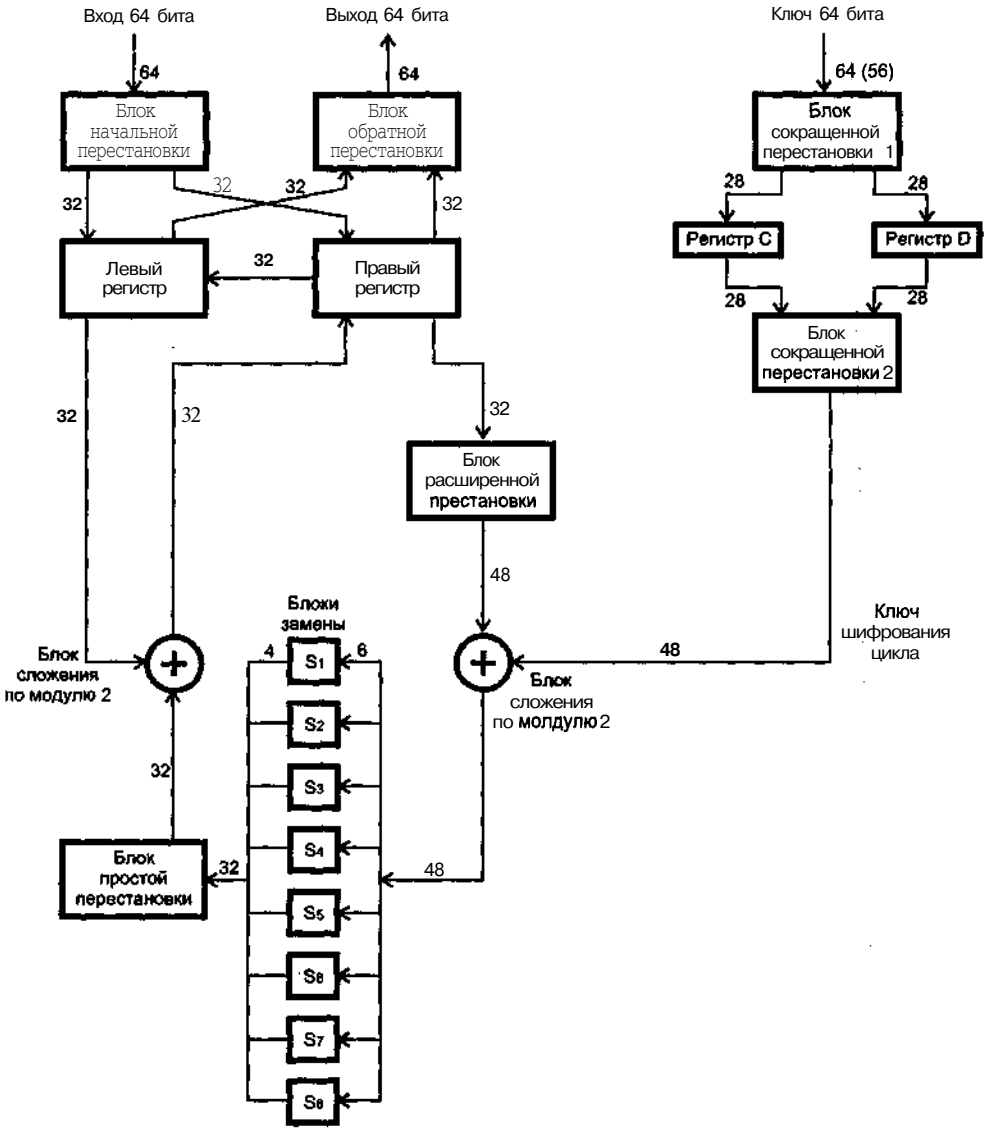


Рис. 4.6. Логическая структурная схема алгоритма шифрования данных DES

Первым преобразованием, которому подвергаются входные данные, является начальная перестановка, имеющая достаточно регулярный характер. Точный порядок замены показан на рис. 4.7. При такой перестановке первый входной бит на выходе становится сороковым, второй — восьмым и т. д. Начальная перестановка используется только для удобства реализации и не имеет самостоятельной криптографической ценности.

После начальной перестановки полученные 64 бита данных делятся на две части по 32 бита, которые записываются в два регистра — левый и правый. Именно после этого и начинается работа основного цикла алгоритма шифрования.

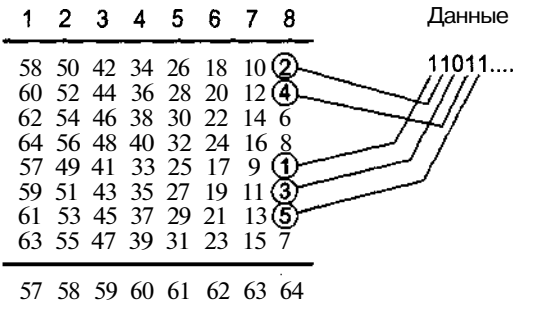


Рис. 4.7. Порядок замены входных данных

Из правого регистра 32 бита поступают на вход блока расширенной перестановки, который производит их регулярное преобразование таким образом, что первый, четвертый, пятый и восьмой биты каждого из четырех октетов преобразуемых бит используются дважды. Таким образом, на выходе блока расширенной перестановки появляется уже не 32, а 48 бит. Правило преобразования данных в блоке расширенной перестановки представлено на рис. 4.8. Как видно из рисунка, при расширенной перестановке 1-й выходной бит соответствует 32-му входному биту, 2-й выходной бит — 1-му входному и т. д.

С выхода блока расширенной перестановки полученные 48 бит данных поступают на сумматор по модулю 2, где складываются с 48 битами ключа шифрования. Полученные в результате этой операции 48 бит данных разделяются на 8 секстетов, поступающих на 8 соответствующих S-блоков замены. С.выходов S-блоков 32 бита (8 раз по 4 бита) поступают на блок простой перестановки, задаваемой табл. 4.1, согласно которой в простой перестановке 1-й выходной бит равен 16-му входному, 2-й выходной бит — 7-му входному и т. д.

Таблица 4.1. Правило простой перестановки

16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

В конце основного цикла данные с выхода блока простой перестановки складываются по модулю 2 с данными, поступившими в левый регистр после начальной перестановки. Результат суммирования поступает в правый регистр, а содержащиеся в нем после начальной перестановки 32 бита без изменений переписываются в левый регистр.

Описанная процедура основного цикла шифрования повторяется 16 раз, прежде чем содержимое правого и левого регистра объединяется в единый 64-битный блок данных и после блока обратной перестановки, осуществляющего перестановку, обратную по отношению к начальной перестановке, поступает на выход алгоритма DES. Отметим, что при формировании 64-битного блока данных, содержимое регистров объединяется в последовательности правого и левого регистров.

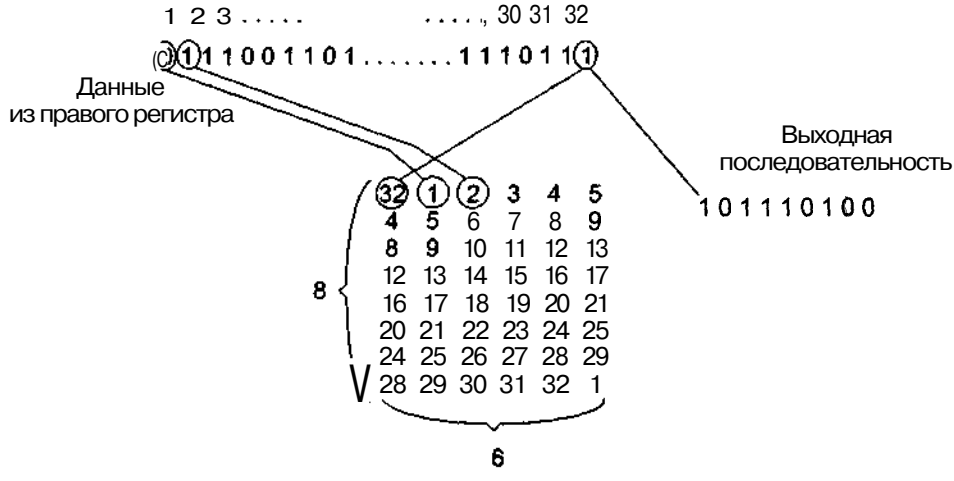


Рис. 4.8. Работа блока расширенной перестановки

Блоки замены в алгоритме DES (в литературе обычно обозначаемые как S-блоки) имеют 6-битные входы и 4-битные выходы. Правило замены в каждом S-блоке определяется соответствующими таблицами S1—S8, представленными ниже.

Первый и последний биты 6-битного входа каждого S-блока задают число в диапазоне от 0 до 3, которое определяет номер строки в таблице замены, биты 2—5 задают число в интервале 0—15, определяя таким образом номер элемента таблицы замены в соответствующей строке. Каждый элемент таблицы замены, представленный в двоичном виде, определяет 4 бита на выходе соответствующего S-блока.

Рассмотрим преобразования, производимые с ключом шифрования до его суммирования с данными, поступающими с выхода блока регистра перестановки. На каждом из 16-и циклов шифрования данные с выхода блока регистра перестановки суммируются с новым ключом шифрования. В правой части рис. 4.6 представлен процесс формирования ключа шифрования для каждого из 16-и циклов.

64 бита исходного ключа преобразуются в первом блоке сокращенной перестановки, где отбрасывается каждый восьмой бит. Если исходный ключ записан в виде 8-и символов кода ASCII, то каждый восьмой отбрасываемый бит является избыточным битом проверки на четность. Результат, полученный в блоке сокращенной перестановки 1, — 56 бит, записывается в регистры C и D, содержащие по 28 бит каждый. Правило перестановки первого блока сокращенной перестановки, с учетом распределения выходных данных по регистрам, задается следующими таблицами:

Регистр C						
57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36

Регистр D						
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

S_2

0	15	1	8	14	6	11	3	4	**9**	7	2	13	12	0	5	10
1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

S_3

0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
1	13	7	0	9	3	4	**6**	10	2	8	5	14	12	11	15	1
2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

S_4

0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
2	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	3	15	0	6	10	1	13	8	**9**	4	5	11	12	7	2	12

S_5

0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
2	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
3	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

S_6

0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
2	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
3	4	3	2	12	9	5	15	10	11	14	1	7	6	0	3	13

S_7

0	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
1	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
2	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
3	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12

S_8

0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

Согласно этим таблицам, первый бит регистра C соответствует 57-му биту исходного ключа шифрования, а первый бит регистра D — 63-му биту ключа шифрования.

Оба регистра обеспечивают возможность циклического сдвига содержащихся в них данных. На каждом цикле алгоритма шифрования производится циклический сдвиг содержимого регистров на 1 или 2 бита влево. Величина сдвига (в битах) на соответствующем цикле задается следующим алгоритмом:

Цикл	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Сдвиг		1		1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

Затем содержимое двух регистров объединяется и подвергается второй сокращенной перестановке, порядок которой задается табл. 4.2. На каждом цикле алгоритма шифрования на выходе сокращенной перестановки образуется ключ шифрования данного цикла.

Таблица 4.2. Порядок второй сокращенной перестановки

14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

Процесс расшифрования аналогичен процессу шифрования, за исключением формирования ключей на соответствующих циклах алгоритма. При этом содержимое регистров C и D сдвигается вправо, а величина сдвига (в битах) задается следующим алгоритмом:

Цикл	1	2	3	4	5	6	7	8	9	10	И	12	13	14	15	16
Сдвиг			0	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

Таким образом, процесс расшифрования является инверсным по отношению к шифрованию данных.

Одна из широко распространенных систем криптографической защиты, использующая стандарт DES, — разработанная в середине 80-х годов прошлого столетия система Kerberos, использование которой предполагает наличие высоконадежного сервера, хранящего исходные копии ключей для взаимодействия с каждым пользователем. Эта система представляет собой часть спецификации открытой вычислительной среды DCE (Distributed Computing Environment) фонда OSF.

Среди предлагающих продукты на базе DCE такие компании, как IBM и Hewlett-Packard. Kerberos должна стать также частью системы защиты Windows NT 5.0. На практике криптографические системы с секретными ключами, как правило, быстрее

систем с открытыми ключами, обеспечивающими ту же степень защиты. Однако преимущество последних в том, что они не позволяют отказаться от авторства, а также обеспечивают проверку целостности сообщений любого сорта.

Система Kerberos (Цербер) обеспечивает защиту сети от несанкционированного доступа, базируясь исключительно на программных решениях, и предполагает многократное шифрование передаваемой по сети управляющей информации. Kerberos обеспечивает идентификацию пользователей сети и серверов, не основываясь на сетевых адресах и особенностях операционных систем рабочих станций пользователей, не требуя физической защиты информации на всех машинах сети и исходя из предположения, что пакеты в сети могут быть легко прочитаны и при желании изменены.

Kerberos имеет структуру типа «клиент-сервер» и состоит из клиентских частей, установленных на всех компьютерах сети (рабочие станции пользователей и серверы), и Kerberos-сервера (или серверов), располагающегося на каком-либо (не обязательно выделенном) компьютере. Kerberos-сервер, в свою очередь, делится на две равноправные части: сервер идентификации (authentication server) и сервер выдачи разрешений (ticket granting server). Следует отметить, что существует и третий сервер Kerberos, который, однако, не участвует в идентификации пользователей, а предназначен для административных целей. Область действия Kerberos (realm) распространяется на тот участок сети, все пользователи которого зарегистрированы под своими именами и паролями в базе Kerberos-сервера и где все серверы обладают общим кодовым ключом с идентификационной частью Kerberos. Эта область не обязательно должна быть участком локальной сети, поскольку Kerberos не накладывает ограничения на тип используемых коммуникаций. Упрощенно модель работы Kerberos можно описать следующим образом.

Пользователь (Kerberos-клиент), желая получить доступ к ресурсу сети, направляет запрос идентификационному серверу Kerberos, который идентифицирует пользователя с помощью его имени и пароля и выдает разрешение на доступ к серверу выдачи разрешений, а тот, в свою очередь, дает разрешение на использование необходимых ресурсов сети. Однако данная модель не отвечает на вопрос о надежности защиты информации, поскольку, с одной стороны, пользователь не может посылать идентификационному серверу свой пароль по сети, а с другой — разрешение на доступ к обслуживанию в сети не может быть послано пользователю в виде обычного сообщения. И *в* том, и в другом случаях информацию можно перехватить и использовать для несанкционированного доступа в сеть. Чтобы избежать подобных неприятностей, Kerberos применяет сложную систему многократного шифрования при передаче любой управляющей информации в сети. Доступ пользователей к сетевым серверам, файлам, приложениям, принтерам и т. д. осуществляется по следующей схеме.

Пользователь (это клиентская часть Kerberos, установленная на рабочей станции пользователя) направляет запрос идентификационному серверу на выдачу «разрешения на получение разрешения» (ticket granting ticket), которое даст возможность обратиться к серверу выдачи разрешений. Идентификационный сервер адресуется к базе данных, хранящей информацию о всех пользователях, и на основании содержащегося в запросе имени пользователя определяет его пароль. Затем клиенту отсылается «разрешение на получение разрешения» и специальный код сеанса (session key), которые шифруются с помощью пароля пользователя, как ключа. При получении этой инфор-

мации пользователь на его рабочей станции должен ввести свой пароль, и если он совпадает с хранящимися в базе Kerberos-сервера, «разрешение на получение разрешения» и код сеанса будут успешно расшифрованы. Таким образом решается проблема с защитой пароля — в данном случае он не передается по сети.

После того как клиент зарегистрировался с помощью идентификационного сервера Kerberos, он отправляет запрос серверу выдачи разрешений на получение доступа к требуемым ресурсам сети. Этот запрос (или «разрешение на получение разрешения») содержит имя пользователя, его сетевой адрес, отметку времени, срок жизни этого разрешения и код сеанса. Запрос зашифровывается два раза: сначала с помощью специального кода, который известен только идентификационному серверу и серверу выдачи разрешений, а затем, как уже было сказано, с помощью пароля пользователя. Это предотвращает не только возможность использования разрешения при его перехвате, но и делает его недоступным самому пользователю. Чтобы сервер выдачи разрешений дал клиенту доступ к требуемым ресурсам, недостаточно только «разрешения на получение разрешения». Вместе с ним клиент посылает так называемый аутентикатор (authenticator), шифруемый с помощью сеансового ключа и содержащий имя пользователя, его сетевой адрес и еще одну отметку времени. Сервер выдачи разрешений расшифровывает полученное от клиента «разрешение на получение разрешения», проверяет, не истек ли срок его «годности», а затем сравнивает имя пользователя и его сетевой адрес, находящиеся в разрешении, с данными, которые указаны в заголовке пакета пришедшего сообщения. Однако на этом проверки не заканчиваются.

Сервер выдачи разрешений расшифровывает аутентикатор с помощью кода сеанса и еще раз сравнивает имя пользователя и его сетевой адрес с предыдущими двумя значениями, и только в случае положительного результата может быть уверен, что клиент именно тот, за кого себя выдает. Поскольку аутентикатор используется для идентификации клиента всего один раз и только в течение определенного периода времени, становится практически невозможным одновременный перехват «разрешения на получение разрешения» и аутентикатора для последующих попыток несанкционированного доступа к ресурсам сети.

Каждый раз при необходимости доступа к серверу сети клиент посылает запрос многоразового использования и новый аутентикатор. После успешной идентификации клиента в качестве источника запроса сервер выдачи разрешений отсылает пользователю разрешение на доступ к ресурсам сети (которое может использоваться многократно в течение некоторого периода времени) и новый код сеанса. Это разрешение зашифровано с помощью кода, известного только серверу выдачи разрешений и серверу, к которому клиент требует доступа, и содержит внутри себя копию нового кода сеанса.

Все сообщение (разрешение и новый код сеанса) зашифровано с помощью старого кода сеанса, поэтому расшифровать его может только клиент. После расшифровки клиент посылает целевому серверу, ресурсы которого нужны пользователю, разрешение на доступ и аутентикатор, зашифрованные с помощью нового кода сеанса. Для обеспечения еще более высокого уровня защиты, клиент, в свою очередь, может потребовать идентификации целевого сервера, чтобы обезопасить себя от возможного перехвата информации, дающей право на доступ к ресурсам сети. В этом случае он

требует от сервера высылки значения отметки времени, увеличенного на единицу и зашифрованного с помощью кода сеанса. Сервер извлекает копию кода сеанса, хранящуюся внутри разрешения на доступ к серверу, использует его для расшифровки аутентикатора, прибавляет к отметке времени единицу, зашифровывает полученную информацию с помощью кода сеанса и отсылает ее клиенту. Расшифровка этого сообщения позволяет клиенту идентифицировать сервер. Использование в качестве кода отметки времени обеспечивает уверенность в том, что пришедший клиенту ответ от сервера не является повтором ответа на какой-либо предыдущий запрос.

Теперь клиент и сервер готовы к передаче необходимой информации с должной степенью защиты. Клиент обращается с запросами к целевому серверу, используя полученное разрешение. Последующие сообщения зашифровываются с помощью кода сеанса.

Более сложной является ситуация, когда клиенту необходимо предоставить серверу право пользоваться какими-либо ресурсами от его имени. В качестве примера можно привести ситуацию, когда клиент посылает запрос серверу печати, которому затем необходимо получить доступ к файлам пользователя, расположенным на файл-сервере. Кроме того, при входе в удаленную систему пользователю необходимо, чтобы все идентификационные процедуры выполнялись так же, как и с локальной машины. Эта проблема решается установкой специальных флажков в «разрешении на получение разрешения» (дающих одноразовое разрешение на доступ к серверу от имени клиента для первого примера и обеспечивающих постоянную работу в этом режиме для второго).

Поскольку разрешения строго привязаны к сетевому адресу обладающей ими станции, то при наличии подобных флажков сервер выдачи разрешений должен указать в разрешении сетевой адрес того сервера, которому передаются полномочия на действия от имени клиента.

Следует отметить также, что для всех описанных выше процедур идентификации необходимо обеспечить доступ к базе данных Kerberos только для чтения. Но иногда требуется изменять базу, например, в случае изменения ключей или добавления новых пользователей. Тогда используется третий сервер Kerberos — административный (Kerberos Administration Server). Не вдаваясь в подробности его работы, отметим, что его реализации могут различаться (так, возможно ведение нескольких копий базы одновременно).

При использовании Kerberos-серверов сеть делится на области действия. Схема доступа клиента, находящегося в области действия одного Kerberos-сервера, к ресурсам сети, расположенным в области действия другого, осуществляется следующим образом.

Оба Kerberos-сервера должны быть обоюдно зарегистрированы, то есть знать общие секретные ключи и, следовательно, иметь доступ к базам пользователей друг друга. Обмен этими ключами между Kerberos-серверами (для работы в каждом направлении используется свой ключ) позволяет зарегистрировать сервер выдачи разрешений каждой области как клиента в другой области. После этого клиент, требующий доступа к ресурсам, находящимся в области действия другого Kerberos-сервера, может получить разрешение от сервера выдачи разрешений своего Kerberos по описанному выше алгоритму.

Это разрешение, в свою очередь, дает право доступа к серверу выдачи разрешений другого Kerberos-сервера и содержит в себе отметку о том, в какой Kerberos-области зарегистрирован пользователь. Удаленный сервер выдачи разрешений использует один из общих секретных ключей для расшифровки этого разрешения (который, естественно, отличается от ключа, используемого в пределах этой области) и при успешной расшифровке может быть уверен, что разрешение выдано клиенту соответствующей Kerberos-области. Полученное разрешение на доступ к ресурсам сети предъявляется целевому серверу для получения соответствующих услуг.

Следует, однако, учитывать, что большое число Kerberos-серверов в сети ведет к увеличению количества передаваемой идентификационной информации при связи между разными Kerberos-областями. При этом увеличивается нагрузка на сеть и на сами Kerberos-серверы. Поэтому более эффективным следует считать наличие в большой сети всего нескольких Kerberos-серверов с большими областями действия, нежели использование множества Kerberos-серверов. Так, Kerberos-система, установленная компанией Digital Equipment для большой банковской сети, объединяющей отделения в Нью-Йорке, Париже и Риме, имеет всего один Kerberos-сервер. При этом, несмотря на наличие в сети глобальных коммуникаций, работа Kerberos-системы практически не отразилась на производительности сети.

К настоящему времени Kerberos выдержал уже пять модификаций. Пятая версия системы Kerberos имеет ряд новых свойств, из которых можно выделить следующие. Уже рассмотренный ранее механизм передачи полномочий серверу на действия от имени клиента, значительно облегчающий идентификацию в сети в ряде сложных случаев, является нововведением пятой версии. Пятая версия обеспечивает упрощенную идентификацию пользователей в удаленных Kerberos-областях с сокращенным числом передач секретных ключей между этими областями. Данное свойство, в свою очередь, базируется на механизме передачи полномочий. Если в предыдущих версиях Kerberos для шифрования был применен исключительно алгоритм DES, надежность которого вызывала некоторые сомнения, то в данной версии возможно использование алгоритмов шифрования, отличных от DES.

Перспективный стандарт AES

Алгоритм шифрования DES давно критикуют за целый ряд недостатков, в том числе, за слишком маленькую длину ключа — всего 56 разрядов. Кроме того, в январе 1999 года закодированное посредством DES сообщение было взломано с помощью связанных через Internet в единую сеть 100 тыс. персональных компьютеров. И на это потребовалось менее 24-х часов. В связи с этим стало очевидным, что в ближайшие несколько лет, учитывая появление более дешевого и высокопроизводительного оборудования, алгоритм DES окажется несостоятельным.

Чтобы решить эту проблему, еще в 1997 году NIST выпустил запрос на комментарий RFC (Request For Comment), где описывался предполагаемый «Усовершенствованный стандарт шифрования» AES (Advanced Encryption Standard), который должен прийти на смену стандарту DES. В 1998 году NIST (National Institute of Standards and Technology), который был предшественником современного Национального институ-

та по стандартам и технологии, объявил конкурс на создание алгоритма, удовлетворяющего требованиям, выдвинутым институтом:

- применение одного или более открытых алгоритмов шифрования;
- общедоступность и отсутствие лицензионных отчислений;
- использование симметричного шифрования;
- поддержка минимального размера блока в 128 разрядов и размеров ключей в 128, 192 и 256 разрядов;
- бесплатное распространение по всему миру;
- приемлемая производительность для различных приложений.

Перед проведением первого тура конкурса в NIST поступило 21 предложение, из которых 15 удовлетворяли выдвинутым критериям. Затем были проведены исследования этих решений, в том числе связанные с дешифровкой и проверкой производительности, и получены экспертные оценки специалистов по криптографии.

В результате в качестве стандарта AES был выбран алгоритм Rijndael, разработанный двумя бельгийскими учеными, специалистами по криптографии. Правительство США объявило, что авторами наиболее перспективного алгоритма шифрования стали Джон Димен из компании Proton World International и Винсент Риджмен, сотрудник Католического университета.

Алгоритм Rijndael является нетрадиционным блочным шифром, поскольку в нем для криптопреобразований не используется сеть Фейштеля. Он представляет каждый блок кодируемых данных в виде таблицы двумерного массива байтов размером 4*4, 4*6 или 4*8 в зависимости от установленной длины блока. Далее, на соответствующих этапах, производятся преобразования либо независимых столбцов, либо независимых строк, либо вообще отдельных байтов в таблице.

Все преобразования в шифре имеют строгое математическое обоснование. Сама структура и последовательность операций позволяют выполнять данный алгоритм эффективно как на 8-битных, так и на 32-битных процессорах. Это позволяет достичь приемлемой производительности при работе на самых разных платформах: от смарт-карт до крупных серверов. В структуре алгоритма заложена возможность параллельного выполнения некоторых операций, что на многопроцессорных рабочих станциях может поднять скорость шифрования еще в 4 раза.

Rijndael представляет собой итеративный блочный шифр, имеющий блоки переменной длины и ключи различной длины. Длина ключа и длина блока может быть 128, 192 или 256 бит независимо друг от друга. Согласно структуре шифра разнообразные преобразования взаимодействуют с промежуточным результатом шифрования, называемым состоянием (state).

Это состояние можно представить в виде прямоугольного массива байтов, который имеет 4 строки, а число столбцов Nb равно длине блока, деленной на 32. Ключ шифрования также представлен в виде прямоугольного массива с четырьмя строками. В этом массиве число столбцов Nk равно длине ключа, деленной на 32. Пример представления состояния и ключа шифрования в виде массивов представлен на рис. 4.9.

В некоторых случаях ключ шифрования показан как линейный массив 4-байтовых слов. Слова состоят из 4-х байт, которые находятся в одном столбце (при представлении в виде прямоугольного массива).

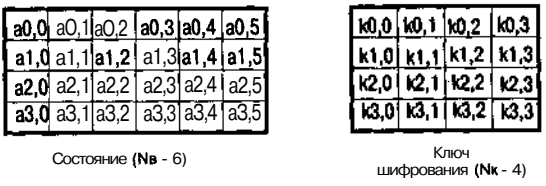


Рис. 4.9. Пример представления состояния (Nb=6) и ключа шифрования (Nk=4) в виде массивов

Входные данные для шифра, например, открытый текст, обозначаются как байты состояния в порядке aO,0, al,0, a3,0, aO,1, a1,1, a3,1 ,a4,1 ... После завершения действия шифра выходные данные получаются из байтов состояния в том же порядке.

Алгоритм состоит из некоторого количества раундов — цикловых преобразований в диапазоне от 10 до 14. Это зависит от размера блока и длины ключа, в которых последовательно выполняются следующие операции:

- замена байт — ByteSub;
- сдвиг строк — ShiftRow;
- замешивание столбцов — MixColumn;
- добавление циклового ключа — AddRoundKey.

Число циклов обозначается Nr и зависит от значений Nb и Nk (рис. 4.10).

Преобразование ByteSub представляет собой нелинейную замену байт, выполняемую независимо с каждым байтом состояния. Порядок замены определяется инвертируемыми S-блоками (таблицами замены), которые построены как композиции двух преобразований:

- получение обратного элемента относительно умножения в поле GF(28);
- применение афинного преобразования (над GF(2)).

Применение преобразования ByteSub к состоянию представлено на рис. 4.11.

Преобразование сдвига строк ShiftRow заключается в том, что последние три строки состояния циклически сдвигаются на различное число байт. При этом первая строка состояния остается без изменения, вторая — сдвигается на C1 байт, третья строка сдвигается на C2 байт, а четвертая — на C3 байт. Значения сдвигов C1, C2 и C3 различны и зависят от длины блока Nb. Величины этих сдвигов в байтах представлены в табл. 4.3

Таблица 4.3. Величина сдвига строк для разной длины блоков

Длина блока, байт	Значение сдвига, байт		
	C_1	C_2	C_3
4	1	2	3
6	1	2	3
8	1	3	4

Nк = 4	10	12	14
Nк = 6	12	12	14
Nк = 8	14	14	14

Рис. 4.10. Число циклов в зависимости от длины ключа и длины блока

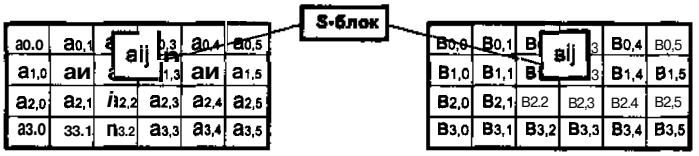


Рис. 4.11. Применение преобразования ByteSub к состоянию

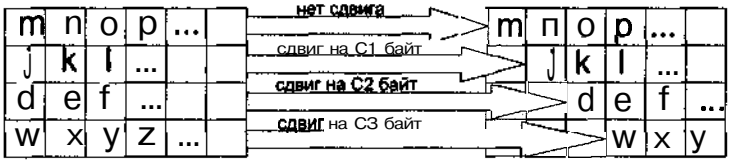


Рис. **4.12.** Пример операции сдвига последних трех строк состояния на определенную величину

Пример операции сдвига последних трех строк состояния на определенную величину представлен на рис. 4.12.

Преобразование замешивания столбцов MixColumn (рис. 4.13) основано на математическом преобразовании, перемещающем данные внутри каждого столбца. В этом преобразовании столбцы состояния рассматриваются как многочлены над GF(28) и умножаются по модулю x4+1 на многочлен C(x).

Операция AddRoundKey — добавление к состоянию циклового ключа посредством простого EXOR. Сам цикловой ключ вырабатывается из ключа шифрования посредством алгоритма выработки ключей (key schedule). Его длина равна длине блока Nb. Преобразование AddRoundKey представлено на рис. 4.14.

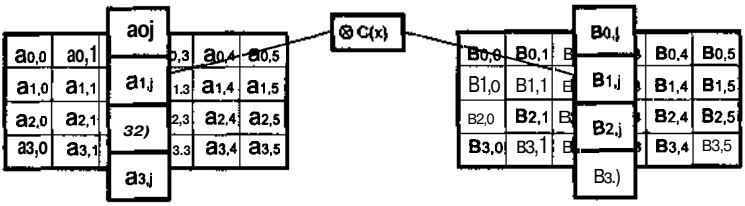


Рис. 4.13. Преобразование замешивания столбцов MixColumn

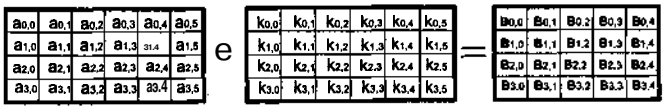


Рис. 4.14. Преобразование AddRoundKey

Алгоритм выработки ключей содержит два этапа:

- расширение ключа (key expansion);
- выбор циклового ключа (round key selection).

В основе алгоритма лежат следующее: общее число бит цикловых ключей равно длине блока, умноженной на число циклов плюс 1. Например, для длины блока 128 бит и 10-и циклов потребуется 1408 бит циклового ключа. Ключ шифрования превращается в расширенный ключ (expanded key). Цикловые ключи выбирают из расширенного ключа так: первый цикловой ключ содержит первые Nb слов, второй — следующие Nb слов и т. д.

Расширенный ключ представляет собой линейный массив 4-битных слов. Первые Nk слов содержат ключ шифрования. Все остальные слова определяются рекурсивно из слов с меньшими индексами, то есть каждое последующее слово получается посредством EXOR предыдущего слова и слова на Nk позиций ранее. Для слов, позиция которых кратна Nk, перед EXOR применяется преобразование к предыдущему слову, а затем еще прибавляется цикловая константа. Преобразование содержит циклический сдвиг байтов в слове, обозначаемый rotl, затем следует применение таблицы замены байт — SubByte. Алгоритм выработки ключей зависит от величины Nk. Расширенный ключ всегда должен получаться из ключа шифрования и никогда не указываться напрямую. При этом нет ограничений на выбор ключа шифрования.

Выбор циклового ключа заключается в том, что каждый цикловой ключ получается из слов массива циклового ключа, как показано для Nb = 6 и Nk = 4 на рис. 4.15.

Выработка ключей может быть сделана и без использования массива. Это характерно для реализаций, в которых критично требование к занимаемой памяти. В этом случае цикловые ключи можно вычислить «на лету» посредством использования буфера из Nk слов.

Теперь рассмотрим особенности реализации алгоритма Rijndael. Этот алгоритм является байт-ориентированным, т. е. полностью может быть сформулирован в терминах операций с байтами. В алгоритме широко используются алгебраические операции в конечных полях, наиболее сложно реализуемо умножение в поле GF(28), Непосредственное выполнение этих операций привело бы к крайне неэффективной реализации алгоритма. Однако байтовая структура шифра открывает широкие возможности для программной реализации. Замена байта по таблице и последующее умножение на константу в конечном поле GF(28) могут быть представлены как одна замена по таблице. Поскольку в прямом шифре используются три константы (01, 02, 03), то понадобятся три такие таблицы, в обратном шифре, соответственно, — четыре (OE, OD, 0B, 09). При надлежащей организации процесса шифрования построчный байтовый сдвиг матрицы данных можно не выполнять. При реализации на 32-битных платформах возможно реализовать байтовую замену и умножение элемента матрицы данных на столбец матрицы M как одну замену 8-и бит на 32 бита.

Таким образом, вся программная реализация раунда шифрования для варианта 128-битных блоков данных сводится к четырем командам загрузки элемента ключа в регистр, шестнадцати командам загрузки байта в регистр и извлечению из памяти индексированного значения. Данное значение используется в операции побитового «исключающего или».

Для процессоров Intel Pentium с недостаточным количеством регистров сюда надо добавить еще 4 команды выгрузки содержимого регистров в память, тогда на указанных процессорах раунд шифрования по алгоритму Rijndael можно выполнить за 40 команд или за 20 тактов процессора с учетом возможности параллельного выполне-

Рис. 4.15. Расширение ключа и выбор циклового ключа

ния команд этим процессором. Для 14 раундов получаем 280 тактов процессора на цикл шифрования плюс несколько дополнительных тактов на «лишнее» прибавление ключа. Добавив несколько тактов на внутрипроцессорные задержки, получим оценку 300 тактов на цикл шифрования. На процессоре Pentium Pro-200 это теоретически позволяет достичь быстродействия примерно 0,67 млн блоков в секунду, или, с учетом размера блока в 128 бит, примерно 8,5 Мбайт/с. Для меньшего числа раундов скорость пропорционально возрастет.

Указанная выше оптимизация потребует, однако, определенных расходов оперативной памяти. Для каждого столбца матрицы M строится свой вектор замены одного байта на 4-байтное слово. Кроме того, для последнего раунда, в котором отсутствует умножение на матрицу M, необходим отдельный вектор замен такого же размера. Это требует использования 5*28*4=5 кбайт памяти для хранения узлов замен для зашифрования и столько же для узлов замен расшифрования — всего 10 кбайт. Для современных компьютеров на базе Intel Pentium под управлением ОС Windows 9x/NT/2000 это не выглядит чрезмерным требованием.

Байт-ориентированная архитектура алгоритма Rijndael позволяет весьма эффективно реализовать его на 8-битных микроконтроллерах, используя только операции загрузки/выгрузки регистров, индексированного извлечения байта из памяти и побитового суммирования по модулю 2. Указанная особенность позволит также выполнить эффективную программную реализацию алгоритма. Раунд шифрования требует выполнения 16-байтных замен плюс четырех операций побитового «исключающего или» над 128-битными блоками, которые можно выполнить *в* три этапа. В итоге получаем 4 операции на раунд, или 57 операций на 14-раундовый цикл шифрования с учетом «лишней» операции побитового прибавления ключа по модулю 2.

Отечественный стандарт шифрования данных ГОСТ 28147-89

Стандарт шифрования ГОСТ 28147-89 также относится к симметричным (одноключевым) криптографическим алгоритмам. Он введен в действие с июля 1990 года и устанавливает единый алгоритм криптографических преобразований для систем обмена информацией в вычислительных сетях, определяет правила шифрования и расшифровки данных, а также выработки имитовставки. Алгоритм в основном удовлетворяет современным криптографическим требованиям, не накладывает ограничений на степень секретности защищаемой информации и обеспечивается сравнительно несложными аппаратными и программными средствами.

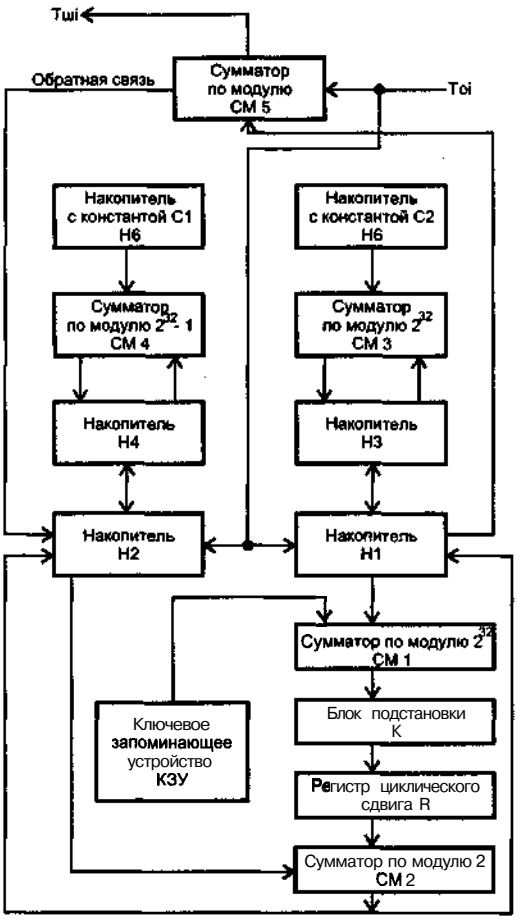


Рис. 4.16. Структурная схема алгоритма криптопреобразования, выполненного по ГОСТ 28147-89

Стандарт шифрования ГОСТ 28147-89 удобен как для аппаратной, так и для программной реализации. При размере блока данных 64 бита основная работа ведется с половинками этого блока (32-битными словами), что позволяет эффективно реализовать указанный стандарт шифрования на большинстве современных компьютеров

Стандарт шифрования ГОСТ 28147-89 предусматривает шифрование и расшифровку данных в следующих режимах работа:

- простая замена;
- гаммирование;
- гаммирование с обратной связью;
- выработка имитовставки.

Структурная схема алгоритма криптопреобразования, выполненного по ГОСТ 28147-89, изображена на рис. 4.16. Эта схема состоит из:

- сумматоров по модулю 2 — СМ2 и СМ5;
- сумматоров по модулю 232 — СМ1 и СМ3;
- сумматора по модулю 232-1 — СМ4;
- накопителей с константами С1 и С2 — Н6 и Н5, соответственно;
- основных 32-разрядных накопителей Н1 и Н2;
- вспомогательных 32-разрядных накопителей Н3 и Н4;
- ключевого запоминающего устройства КЗУ;
- блока подстановки К;
- регистра циклического сдвига R.

Сумматоры по модулю 2 обеспечивают сложение по модулю 2 поступающих на их входы данных, представленных в двоичном виде.

Сумматоры по модулю 232 выполняют операцию суммирования по модулю 232 двух 32-разрядных чисел по правилу:

$A [+] B = A + B$, если $A + B < 232$,

$A [+] B = A + B - 232$, если $A + B > 232$.

Сумматор по модулю 232-1 выполняет операцию суммирования по модулю 232-1 двух 32-разрядных чисел по правилу:

$A [+] B = A + B$, если $A + B < 232-1$,

$A\,[+]\,B = A + B - (232\text{-}1)$, если $A + B > 232\text{-}1$.

Накопители с константами Н6 и Н5 содержат 32-разрядные константы, соответственно,

C1 — 00100000100000001000000010000000;

C2 — 10000000100000001000000010000000.

Основные 32-разрядные накопители служат для обеспечения всех режимов работы алгоритма.

Вспомогательные 32-разрядные накопители используются для обеспечения работы алгоритма в режиме гаммирования.

Ключевое запоминающее устройство предназначено для формирования ключевой последовательности W длиной 256 бит, представленной в виде восьми 32-разрядных чисел Xi (табл. 4.4) [i = 0(1)7]. Последовательность $W = UXi = XO\,U\,X1\,U\,...\,U\,X7$, где U — знак объединения множеств.

Таблица 4.4. Числа, формирующие ключевую последовательность

X_0	32	...	3	2	1
X_1	64	...	35	34	33
X_2	96	...	67	66	65
X_3	128	...	99	98	97
X_4	160	...	129	130	131
X_5	192	...	163	162	161
X_6	224	...	195	194	193
X_7	256	...	227	226	225

Блок подстановки осуществляет дополнительное к ключевой последовательности шифрование передаваемых данных с помощью таблиц замен. Он состоит из восьми узлов замены K1, ... , K8. Поступающий на блок подстановки 32-разрядный вектор разбивается на 8 последовательных 4-разрядных векторов (слов), каждый из которых преобразуется в 4-разрядный вектор соответствующим узлом замены. Узел замены представляет собой таблицу из 16-и строк по 4 бита в каждой (рис. 4.17).

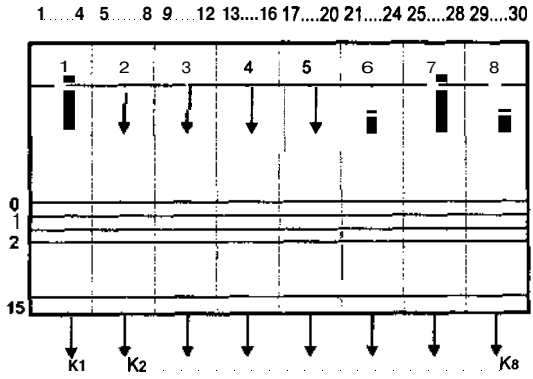


Рис. 4.17. Схема блока подстановки

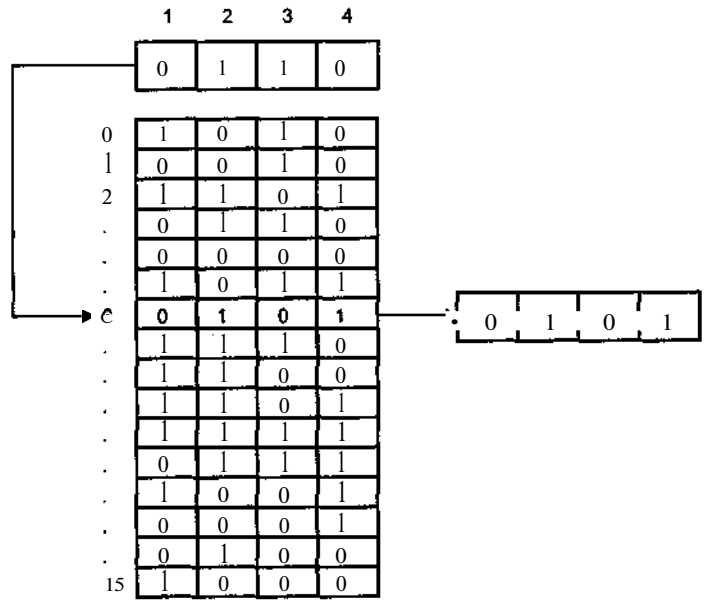


Рис. 4.18. Принцип работы блока подстановки

Входной вектор определяет адрес строки в таблице замены, а заполнение является выходным вектором. Затем выходные 4-разрядные векторы объединяются в один 32-разрядный вектор. Принцип работы блока подстановки рассмотрим на примере, представленном на рис. 4.18.

Пусть имеется блок данных с заполнением 0110. В десятичной системе счисления заполнение 0110 соответствует числу 6. По таблице замен находим строку с номером 6. Результатом является заполнение 0101, соответствующее узлу замены К1.

Таблица блока подстановки содержит набор кодовых элементов, общих для вычислительной сети и практически редко изменяющихся.

Регистр циклического сдвига R предназначен для осуществления операции циклического сдвига шифруемых данных на 11 разрядов в сторону старших разрядов в виде:

R(r32, r31, ... , r2, r1) — (r21, r20, ... , r1, r32, ... , r22)

Заметим, что при суммировании и циклическом сдвиге двоичных векторов старшими считаются разряды накопителей с большими номерами.

Рассмотрим последовательность функционирования алгоритма криптографического преобразования в основных режимах работы.

Режим простой замены

Суть работы алгоритма в режиме простой замены поясним с помощью рис. 4.19.

Открытые данные, предназначенные для шифрования, разбиваются на блоки по 64 бит в каждом, которые обозначим через TOi [i = l(l)m], где m — число 64-разрядных блоков передаваемых открытых данных. После этого выполняются следующие процедуры:

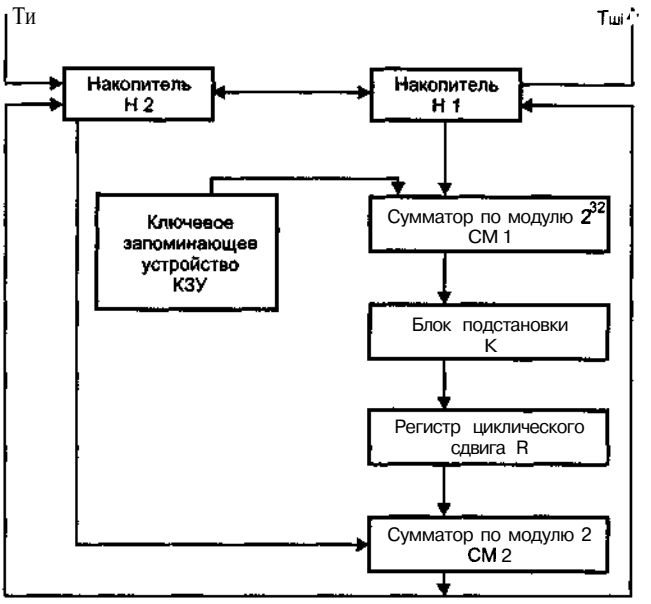


Рис. 4.19. Структурная схема работы алгоритма криптопреобразования в режиме простой замены

- первая последовательность бит T01 разделяется на две последовательности и записывается в накопители: в накопитель H2 — старшие разряды, в накопитель H1 — младшие разряды;
- в ключевое запоминающее устройство вводится ключевая последовательность длиной 256 бит;
- выполняется итеративный процесс шифрования, состоящий из 32-х циклов.

Первый цикл происходит в следующей последовательности:

1. Содержимое накопителя H1 суммируется по модулю 232 в сумматоре СМ1 с содержимым строки XO из ключевого запоминающего устройства.

2. Результат суммирования из сумматора СМ1 поступает на блок подстановки, где происходит поблочная замена результата по 4 бита в таблице замен.

3. С выхода блока подстановки шифруемые данные сдвигаются на 11 разрядов влево в регистре сдвига и поступают на сумматор СМ2.

Рис. 4.20. Ключи, соответствующие каждому циклу шифрования

4. В сумматоре СМ2 содержимое регистра сдвига складывается по модулю 2 с содержимым накопителя Н2.

5. Начальное содержимое накопителя Н1 поступает в накопитель Н2, а результат суммирования в сумматоре СМ2 заносится в накопитель Н1.

Следующие 31 цикл аналогичны первому, за исключением того, что для выполнения очередного цикла из ключевого запоминающего устройства выбирается ключ в последовательности, представленной на рис. 4.20.

После выполнения 32-го, последнего цикла, полученный результат из сумматора СМ2 поступает в накопитель Н2, а в накопителе Н1 сохраняется результат предыдущего цикла. Информация, содержащаяся в накопителях Н1 и Н2, представляет собой первый 64-разрядный блок зашифрованных данных. Остальные блоки открытых данных шифруются в режиме простой замены аналогично.

При расшифровке закрытых данных порядок выбора ключей из ключевого запоминающего устройства происходит в обратной последовательности.

Режим гаммирования

Режим гаммирования заключается в том, что открытые данные, предварительно разбитые на 64-битные блоки, поразрядно складываются по модулю 2 с гаммой шифра Гш, представляемой в виде 64-битных блоков:

Гш={Г1, Г2, ... , Гm}={Гi}m, [i=l(l)m],

где т — количество 64-разрядных блоков, определяемое длиной шифруемого сообщения.

Процесс шифрования данных в рассматриваемом режиме работы алгоритма поясним с помощью рис. 4.16.

В ключевое запоминающее устройство вводится ключевая последовательность длиной 256 бит и формируется синхропосылка S в виде 64-разрядной двоичной последовательности S = {S1, ... , S64} = {Si}64, которая записывается в накопители Н1 и Н2 следующим образом:

- S1 — в первый разряд накопителя Н1;
- S2 — во второй разряд накопителя Н2;
- ...;
- S32 — в 32-й разряд накопителя Н1;
- S33 — в первый разряд накопителя Н2;
- ...;
- S64 — в 32-й разряд накопителя Н2.

Полученная синхропосылка S затем шифруется в режиме простой замены. Результат шифрования из накопителя Н1 переписывается в накопитель Н3, а из накопителя Н2 — в накопитель Н4.

Содержимое накопителя Н4 суммируется по модулю 232-1 с константой С1 в сумматоре СМ4, результат суммирования записывается в накопитель Н4.

Содержимое накопителя Н3 суммируется по модулю 232 с константой С2 в сумматоре СМ3, результат суммирования записывается в накопитель Н3.

Далее содержимое накопителя Н4 переписывается в накопитель Н2, а содержимое накопителя Н3 — в накопитель Н1. Полученные таким образом данные в накопителях Н1 и Н2 шифруются в режиме простой замены, а результатом шифрова-

ния является формирование в этих же накопителях 64-разрядного блока гамма-шифра Г1.

Полученный гамма-шифр Г1 суммируется поразрядно по модулю 2 с первым 64-разрядным блоком открытых данных Т01 в сумматоре СМ5. Результат суммирования — первый 64-разрядный блок зашифрованных данных Тш1.

Шифрование второго и последующих блоков открытых данных осуществляется с помощью формирования второго и последующих гамма-шифров в соответствии с рассмотренными преобразованиями режима простой замены. Если в последнем m блоке открытых данных число двоичных разрядов меньше 64, неиспользованная часть гамма-шифра Гш просто отбрасывается.

Расшифровка данных выполняется в обратной последовательности на основе знания ключевой последовательности и синхропосылки S, которая не является секретным элементом шифрования и может храниться в запоминающем устройстве или передаваться в незащищенном виде по каналам связи.

Режим гаммирования с обратной связью

Принцип работы алгоритма в режиме гаммирования с обратной связью отличается от принципа работы предыдущего режима тем, что если на первом шаге при формировании гамма-шифра используется синхропосылка, то на всех последующих шагах — предыдущий блок зашифрованных данных. За счет этого достигается сцепление блоков шифруемых данных: каждый блок данных при шифровании зависит от всех предыдущих.

Шифрование открытых данных в этом режиме происходит по той же схемной реализации, что и в режиме гаммирования, и отличается лишь введением дополнительной обратной связи с выхода сумматора СМ5 на входы накопителей Н1 и Н2.

Для пояснения процесса шифрования данных в режиме гаммирования с обратной связью вновь обратимся к рис. 4.16 и приведем последовательность выполняемых процедур.

В ключевое запоминающее устройство вводится ключевая последовательность длиной 256 бит, после чего формируется синхропосылка S, записываемая в накопители Н1 и Н2, содержимое которых шифруется в режиме простой замены. Результат шифрования в накопителях Н1 и Н2 представляет собой первый 64-разрядный блок гамма-шифра П.

Полученный гамма-шифр Г1 суммируется поразрядно по модулю 2 с первым 64-разрядным блоком открытых данных Т01 в сумматоре СМ5. Результат суммирования — первый 64-разрядный блок зашифрованных данных Тш1. Первый блок зашифрованных данных Тш1 по обратной связи поступает на накопители Н1 и Н2 и является исходной информацией для формирования второго блока гамма-шифра Г2.

Содержимое накопителей Н1 и Н2 шифруется в режиме простой замены. Результат шифрования в накопителях Н1 и Н2 представляет второй 64-разрядный блок гамма-шифра Г2. Этот гамма-шифр суммируется по модулю 2 поразрядно со вторым 64-разрядным блоком открытых данных Т02 в сумматоре СМ5. В результате получается второй 64-разрядный блок зашифрованных данных Тш2 и т. д. Если в последнем m блоке открытых данных Тот число двоичных разрядов меньше 64, неиспользованная часть гамма-шифра отбрасывается.

Расшифровка данных происходит в обратном порядке на основе знания ключевой последовательности и синхропосылки S.

Режим выработки имитовставки

Режим выработки имитовставки предназначен для обнаружения случайных и преднамеренных ошибок при передаче шифрованных данных потребителям и одинаков для любого из режимов шифрования открытых данных.

Имитовставка представляет собой дополнительный блок данных U из L бит, который формируется либо перед шифрованием всего сообщения, либо совместно с шифрованием по блокам. Число двоичных разрядов L в имитовставке определяется криптографическими требованиями с учетом вероятности возникновения ложной имитовставки:

$Po = 2 - L$.

Первые блоки открытых данных, которые участвуют в формировании имитовставки, как правило, содержат служебную информацию (адресную часть, время, синхропосылку) и не зашифровываются.

Процесс формирования имитовставки поясним также с помощью рис. 4.16.

Как и в рассмотренных выше режимах, в ключевое запоминающее устройство вводится ключевая последовательность длиной 256 бит. Далее первый 64-разрядный блок открытых данных To1 поступает в накопители H1 и H2, содержимое которых подвергается преобразованию, соответствующему первым 16-и циклам итеративного процесса шифрования в режиме простой замены. Результат шифрования в режиме простой замены с накопителей H1 и H2 суммируется по модулю 2 со вторым блоком открытых данных To2 в сумматоре CM5.

Результат суммирования из сумматора CM5 поступает в накопители H1 и H2 и после 16-и циклов шифрования в режиме простой замены суммируется по модулю 2 с третьим блоком открытых данных в сумматоре CM5 и т. д.

Последний 64-разрядный блок открытых данных T0m, дополненный при необходимости до полного 64-разрядного числа нулями, суммируется по модулю 2 с результатом работы алгоритма на (m-1) шаге в сумматоре CM5 и снова зашифровывается по первым 16-и циклам режима простой замены.

Из полученного таким образом последнего заполнения накопителей H1 и H2 выбирается имитовставка U длиной L бит. В большинстве практических случаев в качестве имитовставки используется содержимое накопителя H1 (32 младших бита последнего блока зашифрованных данных).

Имитовставка U передается по каналам связи в конце зашифрованных данных или после каждого шифрованного блока. Поступившие данные расшифруются и из полученных блоков открытых данных T0i вырабатывается имитовставка U, которая сравнивается с имитовставкой, полученной по каналу связи. В случае несовпадения имитовставок расшифрованные данные считают ложными.

Познакомившись с принципом работы криптографического алгоритма ГОСТ 28147-89, рассмотрим его эффективность и практическую реализацию.

Российский стандарт шифрования ГОСТ 28147-89 удобен как для аппаратной, так и для программной реализации. При размере блока данных 64 бита основная работа ведется с половинками этого блока — 32-битными словами, что позволяет эффективно реализовать российский стандарт шифрования на большинстве современных компьютеров. При реализации на 32-битных машинах наиболее трудоемка операция замены. Предусмотренные ГОСТом подстановки в 4-битных группах при программной

реализации дают возможность попарно объединить и выполнить замену в 8-битных группах, что существенно эффективнее. Надлежащая организация замены позволяет также избежать вращения слова на выходе функции шифрования, если хранить узлы замены как массивы 4-байтовых слов, в которых уже выполнено вращение.

Такая «раздутая» таблица замен потребует для своего хранения 4*28*4 = 212 байт или 4K оперативной памяти. Указанные шаги оптимизации позволяют реализовать раунд шифрования по ГОСТу за 10 машинных команд, включая выделение и загрузку в регистры отдельных байтов из 4-байтовых слов. С учетом способности процессоров Intel Pentium параллельно выполнять команды, раунд ГОСТа может быть реализован за 6 тактов работы процессора, а весь процесс шифрования — за 32*6 = 192 такта. Добавляя еще 8 тактов на различные внутрипроцессорные задержки, получим оценку затрат процессорного времени на реализацию цикла шифрования по алгоритму ГОСТ 28147-89 в 200 тактов. На процессоре Pentium Pro 200 это позволит достичь предела быстродействия шифрования миллион блоков в секунду, или 8 Мбайт/с (на самом деле эта величина будет меньше).

Рассматриваемый алгоритм шифрования может быть также эффективно реализован и на 8-битных микроконтроллерах, поскольку составляющие его элементарные операции входят в систему команд большинства наиболее распространенных контроллеров. При этом суммирование по модулю 232 придется разделить на одну операцию сложения без переноса и три операции сложения с переносом, выполняемые каскадно. Все остальные операции также легко могут быть представлены в виде 8-байтовых операндов.

При аппаратной реализации ГОСТа один раунд предполагает последовательное выполнение трех операций над 32-битными аргументами: суммирование, замена, выполняемая одновременно во всех восьми 4-битных группах, и побитовое суммирование по модулю 2. Циклический сдвиг не является отдельной операцией, так как обеспечивается простой коммутацией проводников. Таким образом, при аппаратной реализации цикл шифрования требует выполнения 106 элементарных операций, и эту работу нельзя распараллелить.

Характеристики быстродействия программных реализаций, выполненных по алгоритму ГОСТ 28147-89 и новому американскому стандарту шифрования — шифру Rijndael, представлены в табл. 4.5.

Таблица 4.5. Показатели быстродействия реализаций алгоритмов шифрования

Процессор	ГОСТ 28147-89	Rijndael, 14 раундов
Pentium 166	2,04 Мбайт/с	2,46 Мбайт/с
Pentium III 433	8,30 Мбайт/с	9,36 Мбайт/с

Из табл. 4.5 видно, что рассмотренные алгоритмы обладают сопоставимыми характеристиками быстродействия при реализации на 32-битных платформах. При использовании 8-битных платформ картина будет примерно такой же.

Что касается аппаратной реализации, то, в отличие от алгоритмов шифрования ГОСТа, Rijnael позволяет достичь высокой степени параллелизма при выполнении шифрования, оперирует блоками меньшего размера и содержит меньшее число раундов, в силу чего его аппаратная реализация на базе одной и той же технологии теоретически может быть более быстродействующей (примерно в 4 раза).

Проведенное выше сопоставление параметров алгоритмов шифрования ГОСТ28147-89 и Rijndael показывает, что, несмотря на существенное различие архитектурных принципов, на которых базируются шифры, их основные рабочие параметры примерно одинаковы. Исключением является то, что, по всей вероятности, Rijnael будет иметь определенное преимущество в быстродействии перед ГОСТом при аппаратной реализации на базе одной и той же технологии. По ключевым параметрам криптостойкости для алгоритмов такого рода ни один из них не обладает значительным преимуществом; примерно одинаковы и скорости оптимальной программной реализации для процессоров Intel Pentium, что можно экстраполировать на все современные 32-разрядные процессоры. Таким образом, можно сделать вывод, что отечественный стандарт шифрования соответствует требованиям, предъявляемым к современным шифрам, и может оставаться стандартом еще достаточно долгое время. Очевидным шагом в его оптимизации может стать переход от замен в 4-битных группах к байтовым заменам, за счет чего должна возрасти устойчивость алгоритма к известным видам криптоанализа.

Система PGP — мировой стандарт доступности

Много лет назад проблема защиты частной жизни граждан не стояла так уж остро, в связи с тем, что вмешаться в личную жизнь было технически достаточно трудно (труд этот был, как мы можем сейчас сказать, не автоматизирован). В настоящее время благодаря развитию информационных технологий компьютеры могут делать то, что не всегда могут делать люди, в частности, искать в речевых или текстовых фрагментах определенные ключевые фразы. И не только это. Теперь стало гораздо легче перехватывать информацию, особенно в сети Internet, которая общедоступна и содержит множество точек, где сообщения можно перехватить. Организации и фирмы, которые могут себе позволить тратить крупные средства на защиту своей информации, применяют сложные дорогостоящие системы шифрования, строят свои службы безопасности, используют специальные технические средства и т. п.

Алгоритмы шифрования реализуются программными или аппаратными средствами. Существует великое множество чисто программных реализаций различных алгоритмов. Из-за своей дешевизны (некоторые из них и вовсе распространяются бесплатно), а также высокого быстродействия процессоров, простоты работы и безотказности они вполне конкурентоспособны. В этой связи нельзя не упомянуть программный пакет PGP (Pretty Good Privacy), в котором комплексно решены практически все проблемы защиты передаваемой информации. Благодаря PGP рядовые граждане могут достаточно надежно защищать свою информацию, причем с минимальными затратами.

Система PGP, начиная с 1991 года, остается самым популярным и надежным средством криптографической защиты информации всех пользователей сети Internet. Сила PGP состоит в превосходно продуманном и чрезвычайно мощном механизме обработки ключей, быстроте, удобстве и широте их распространения. Существуют десятки не менее сильных алгоритмов шифрования, чем тот, который используется в PGP, но популярность и бесплатное распространение сделали PGP фактическим стандартом для электронной переписки во всем мире.

Программа PGP разработана в 1991 году Филиппом Зиммерманом (Philip Zimmermann). В ней применены сжатие данных перед шифрованием, мощное управ-

ление ключами, вычисление контрольной функции для цифровой подписи, надежная генерация ключей.

В основе работы PGP лежат сразу два криптоалгоритма — обычный алгоритм шифрования с закрытым ключом и алгоритм шифрования с открытым ключом (рис. 4.21). Зачем это нужно? Алгоритм шифрования с закрытым ключом требует защищенного канала для передачи этого самого ключа (ведь одним и тем же ключом можно как зашифровать, так и расшифровать сообщение). Система с открытым ключом позволяет распространять ключ для зашифровки сообщения совершенно свободно (это и есть открытый ключ), однако расшифровать сообщение можно при помощи второго, закрытого ключа, который хранится только у пользователя. Более того, это справедливо и в обратную сторону — расшифровать сообщение, зашифрованное закрытым ключом, можно только при помощи открытого ключа. Недостатком данного алгоритма является крайне низкая скорость его выполнения.

Однако, при шифровании сообщения в PGP оба эти ограничения обойдены достаточно оригинальным способом. Вначале генерируется случайным образом ключ для алгоритма с закрытым ключом (кстати, в качестве такого алгоритма используется очень стойкий алгоритм IDEA). Ключ этот генерируется только на один сеанс, причем таким образом, что повторная генерация того же самого ключа практически невозможна. После зашифровки сообщения к нему прибавляется еще один блок, в котором содержится данный случайный ключ, но уже зашифрованный при помощи открытого ключа алгоритма с открытым ключом RSA. Таким образом, для расшифровки необходимо и достаточно знать закрытый ключ RSA.

Для пользователя все это выглядит гораздо проще: он может зашифровать сообщение общедоступным открытым ключом и отправить это сообщение владельцу закрытого ключа. И только этот владелец и никто иной сможет прочесть сообщение. При этом программа PGP работает очень быстро. Как же она это делает?

Когда пользователь шифрует сообщение с помощью PGP, программа сначала сжимает текст, убирая избыточность, что сокращает время на отправку сообщения через модем и повышает надежность шифрования. Большинство приемов криптоанализа (взлома зашифрованных сообщений) основаны на исследовании «рисунков», присущих текстовым файлам. Путем сжатия эти «рисунки» ликвидируются. Затем программа PGP генерирует сессионный ключ, который представляет собой случайное число, созданное за счет движений вашей мыши и нажатий клавиш клавиатуры.

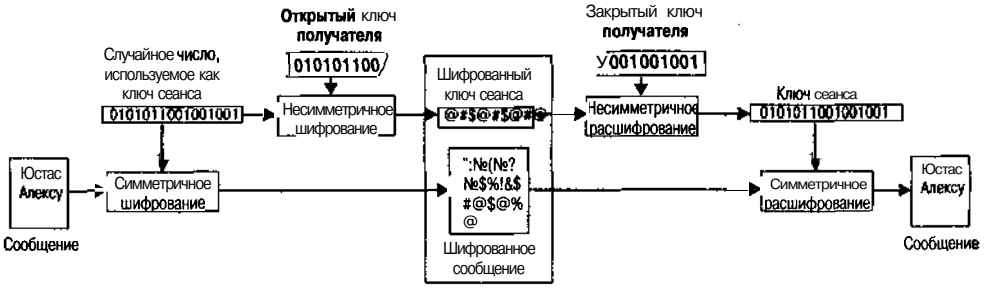


Рис. 4.21. Принцип работы криптоалгоритма PGP

Как только данные будут зашифрованы, сессионный ключ зашифровывается с помощью открытого ключа получателя сообщения, который отправляется к получателю вместе с зашифрованным текстом.

Расшифровка происходит в обратной последовательности. Программа PGP получателя сообщения использует закрытый ключ получателя для извлечения временного сессионного ключа, с помощью которого программа затем дешифрует текст.

Тем не менее при работе с программой PGP возникает проблема: при шифровании исходящих сообщений открытым ключом своего корреспондента, отправитель сообщений не может их потом прочитать, ввиду того, что исходящее сообщение шифруется с помощью закрытого ключа отправителя и открытого ключа его корреспондента Чтобы этого избежать, в настройках программы PGP есть опция, позволяющая зашифровывать свои исходящие сообщения таким образом, чтобы их можно было потом взять из архива и прочитать.

Ключи, используемые программой, хранятся на жестком диске компьютера в зашифрованном состоянии в виде двух файлов, называемых кольцами (keyrings): одного для открытых ключей, а другого — для закрытых. В течение работы с программой PGP открытые ключи корреспондентов вносятся в открытые кольца. Закрытые ключи хранятся в закрытом кольце. Если вы потеряли закрытое кольцо, то не сможете расшифровать информацию, зашифрованную с помощью ключей, находящихся в этом кольце.

Хотя открытый и закрытый ключи взаимосвязаны, чрезвычайно сложно получить закрытый ключ, исходя из наличия только открытого ключа, однако это возможно, если вы имеете мощный компьютер. Поэтому крайне важно выбирать ключи подходящего размера: достаточно большого для обеспечения безопасности и достаточно малого для обеспечения быстрого режима работы. Кроме этого, необходимо учитывать личность того, кто намеревается прочитать ваши зашифрованные сообщения, насколько он заинтересован в их расшифровке, каким временем он располагает и какие у него имеются ресурсы.

Более длинные ключи будут более надежными в течение длительного срока. Поэтому, если вам необходимо так зашифровать информацию, чтобы она хранилась в течение нескольких лет, следует применить мощный ключ.

Открытые ключи для шифрования можно разместить на одном из PGP-серверов. С этого момента каждый, кто хочет, может послать вам электронную почту в зашифрованном виде. Если вы используете преимущественно одну и ту же почтовую программу, шифрование и дешифровка будут не сложнее простого нажатия кнопки. Если же вы используете разные программы, то достаточно поместить письмо в буфер и дать команду шифровать в буфере. После этого можно вернуть письмо в почтовую программу и отослать. Существуют три основных способа шифрования информации:

G напрямую в почтовой программе (самый удобный);

- через копирование текста в буфер обмена Windows;
- через шифрование всего файла, который затем прикрепляется к сообщению.

Программа PGP предназначена, в первую очередь, для защиты электронной почты, хотя ее можно использовать и для защиты файлов на жестком диске. Особенно привлекательными чертами PGP являются многочисленные plug-ins для таких популярных почтовых программ, как Eudora, Netscape и Outlook. Plug-ins настраивают PGP

для этих программ и дополняют их некоторыми приятными мелочами, например, дополнительными кнопками на панели инструментов. Пиктограмма в правом нижнем углу (tray), всплывающая панель инструментов (floating toolbox) и меню правой кнопки мыши (right-click menu) в PGP очень логичны и удобны, поэтому она проста в управлении.

Можно столкнуться с системой защиты PGP в программе Nuts & Bolts фирмы Helix Software. Это та же программа, только PGP — более новой версии. Компания Network Associates поглотила Helix и завладела правами на продукт. Новая версия PGP for Personal Privacy совместима с предыдущими версиями, в том числе Nuts & Bolts.

Рекомендуется использовать связку популярной почтовой программы The Bat! (заодно поддержав производителей отечественного программного обеспечения) и PGP. Безусловным достоинством этой программы является то, что она позволяет использовать как внешнюю программу PGP (то есть оригинальную, непосредственно от разработчиков), так и установить специальное дополнение к программе, дающее возможность работать с PGP (основанное на популярной библиотеке SSLeay). Все основные возможности PGP поддерживаются в полной мере и достаточно просты в употреблении.

Заметим, что PGP позволяет шифровать сообщение и составлять электронную подпись (ее еще часто называют сигнатурой или PGP-сигнатурой). Если с шифрованием все достаточно понятно, то сигнатура нуждается в дополнительном пояснении. Все дело в том, что сообщение может быть не только прочтено, но и модифицировано. Для установки факта целостности сообщения вычисляется дайджест сообщения — аналог контрольной суммы, но более надежный в силу его уникальности.

Программа PGP применяет так называемую **хэш-функцию**. Ее работа заключается в следующем. Если произошло какое-либо изменение информации, пусть даже на один бит, результат хэш-функции будет совершенно иным. Дайджест шифруется при помощи закрытого ключа и прилагается к самому сообщению. Теперь получатель может при помощи открытого ключа расшифровать дайджест отправителя, затем, вычислив заново дайджест для полученного сообщения, сравнить результаты. Полное совпадение дайджестов говорит о том, что сообщение не изменилось при пересылке.

Шифрование и электронную подпись можно использовать и одновременно. В этом случае отправитель при помощи открытого ключа получателя шифрует сообщение, а потом подписывает его при помощи своего закрытого ключа. В свою очередь получатель сначала проверяет целостность сообщения, применяя открытый ключ отправителя, а потом расшифровывает сообщение, используя уже собственный закрытый ключ. Все это кажется достаточно сложным, однако на практике усваивается быстро. Достаточно обменяться с кем-нибудь парой писем с помощью PGP.

В настоящий момент программа доступна на платформах UNIX, DOS, Macintosh и VAX. Пакет программ PGP свободно распространяется по Internet для некоммерческих пользователей вместе с 75-страничным справочным руководством.

Однако следует сразу предупредить пользователей, что система PGP не сертифицирована для применения в Российской Федерации. Поэтому следует избегать ее использования в государственных организациях, коммерческих банках и т. п. Но для личного пользования граждан она является великолепным средством защиты от посягательств на свою частную жизнь.

Криптографические ключи

Известно, что все без исключения алгоритмы шифрования используют криптографические ключи. Именно поэтому одна из задач криптографии — управление ключами, т. е. их генерация, накопление и распределение. Если в компьютерной сети зарегистрировано п пользователей и каждый может связаться с каждым, то для нее необходимо иметь п*(п-1)/2 различных ключей. При этом каждому из п пользователей следует предоставить (n–1) ключ, т. к. от их выбора в значительной степени зависит надежность защиты конфиденциальной информации. Выбору ключа для криптосистемы придается особое значение.

Более того, так как практически любой криптографический ключ может быть раскрыт злоумышленником, то необходимо использовать определенные правила выбора, генерации, хранения и обновления их в процессе сеансов обмена секретными сообщениями, а также их доставки безопасным способом до получателей. Также известно, что для одноключевых криптосистем необходим защищенный канал связи для управления ключом. Для двухключевых криптосистем нет необходимости в таком канале связи.

Процесс генерации ключей должен быть случайным. Для этого можно использовать генераторы случайных чисел, а также их совокупность с каким-нибудь непредсказуемым фактором, например, выбором битов от показаний таймера. При накоплении ключи нельзя записывать в явном виде на носители. Для повышения безопасности ключ должен быть зашифрован другим ключом, другой — третьим и т. д. Последний ключ в этой иерархии шифровать не нужно, но его следует размещать в защищенной части аппаратуры. Такой ключ называется мастер-ключом.

Выбранные ключи необходимо распределять таким образом, чтобы не было закономерностей в изменении ключей от пользователя к пользователю. Кроме того, надо предусмотреть частую смену ключей, причем частота их изменения определяется двумя факторами: временем действия и объемом информации, закрытой с их использованием.

Выбор длины криптографического ключа

Криптографические ключи различаются по своей длине и, следовательно, по силе: ведь чем длиннее ключ, тем больше число возможных комбинаций. Скажем, если программа шифрования использует 128-битные ключи, то ваш конкретный ключ будет одной из 2128 возможных комбинаций нулей и единиц. Злоумышленник с большей вероятностью выиграет в лотерею, чем взломает такой уровень шифрования методом «грубой силы» (т. е. планомерно перебирая ключи, пока не встретится нужный). Для сравнения: чтобы подобрать на стандартном компьютере симметричный 40-битный ключ, специалисту по шифрованию потребуется около 6 часов. Даже шифры со 128-битным ключом до некоторой степени уязвимы, т. к. профессионалы владеют изощренными методами, которые позволяют взламывать даже самые сложные коды.

Надежность симметричной криптосистемы зависит от стойкости используемого криптографического алгоритма и от длины секретного ключа. Допустим, что сам алгоритм идеален: вскрыть его можно только путем опробования всех возможных клю-

чей. Этот вид криптоаналитической атаки называется методом тотального перебора. Чтобы применить данный метод, криптоаналитику понадобится немного шифротекста и соответствующий открытый текст. Например, в случае блочного шифра ему достаточно получить в свое распоряжение по одному блоку шифрованного и соответствующего открытого текста. Сделать это не так уж и трудно.

Криптоаналитик может заранее узнать содержание сообщения, а затем перехватить его при передаче в зашифрованном виде. По некоторым признакам он также может догадаться, что посланное сообщение представляет собой не что иное, как текстовый файл, подготовленный с помощью распространенного редактора, компьютерное изображение в стандартном формате, каталог файловой подсистемы или базу данных. Для криптоаналитика важно то, что в каждом из этих случаев в открытом тексте перехваченного шифросообщения известны несколько байт, которых ему хватит, чтобы предпринять атаку.

Подсчитать сложность атаки методом тотального перебора достаточно просто. Если ключ имеет длину 64 бита, то суперкомпьютер, который может опробовать 1 млн ключей за 1 с, потратит более 5000 лет на проверку всех возможных ключей. При увеличении длины ключа до 128 бит этому же суперкомпьютеру понадобится 1025 лет, чтобы перебрать все ключи. Можно сказать, что 1025 — это достаточно большой запас надежности для тех, кто пользуется 128-битными ключами.

Однако прежде чем броситься спешно изобретать криптосистему с длиной ключа, например, в 4000 байт, следует вспомнить о сделанном выше предположении: используемый алгоритм шифрования идеален в том смысле, что вскрыть его можно только методом тотального перебора. Убедиться в этом на практике бывает не так просто, как может показаться на первый взгляд.

Криптография требует утонченности и терпения. Новые сверхсложные криптосистемы при более внимательном рассмотрении часто оказываются очень нестойкими. А внесение даже крошечных изменений в стойкий криптографический алгоритм может существенно понизить его стойкость. Поэтому надо пользоваться только проверенными шифрами, которые известны уже в течение многих лет, и не бояться проявлять болезненную подозрительность по отношению к новейшим алгоритмам шифрования, вне зависимости от заявлений их авторов об абсолютной надежности этих алгоритмов.

Важно также не забывать о том, что стойкость алгоритма шифрования должна определяться ключом, а не деталями самого алгоритма. Чтобы быть уверенным в стойкости используемого шифра, недостаточно проанализировать его при условии, что противник досконально знаком с алгоритмом шифрования. Нужно еще и рассмотреть атаку на этот алгоритм, при которой враг может получить любое количество шифрованного и соответствующего открытого текста. Более того, следует предположить, что криптоаналитик имеет возможность организовать атаку с выбранным открытым текстом произвольной длины.

К счастью, в реальной жизни большинство людей, интересующихся содержанием ваших шифрованных файлов, не обладают квалификацией высококлассных специалистов и необходимыми вычислительными ресурсами, которые имеются в распоряжении правительств мировых супердержав. Последние же вряд ли будут тратить время и деньги, чтобы прочесть ваше пылкое сугубо личное послание. Однако, если вы плани-

руете свергнуть «антинародное правительство», вам необходимо всерьез задуматься о стойкости применяемого алгоритма шифрования.

Многие современные алгоритмы шифрования с открытым ключом основаны на однонаправленности функции разложения на множители числа, являющегося произведением двух больших простых чисел. Эти алгоритмы также могут быть подвергнуты атаке, подобной методу тотального перебора, применяемому против шифров с секретным ключом, с одним лишь отличием: опробовать каждый ключ не потребуется, достаточно суметь разложить на множители большое число.

Конечно, разложение большого числа на множители — задача трудная. Однако сразу возникает резонный вопрос, насколько трудная. К несчастью для криптографов, ее решение упрощается, и, что еще хуже, значительно более быстрыми темпами, чем ожидалось. Например, в середине 70-х годов считалось, что для разложения на множители числа из 125 цифр потребуются десятки квадрильонов лет. А всего два десятилетия спустя с помощью компьютеров, подключенных к сети Internet, удалось достаточно быстро разложить на множители число, состоящее из 129 цифр. Этот прорыв стал возможен благодаря тому, что за прошедшие 20 лет были не только предложены новые, более быстрые, методы разложения на множители больших чисел, но и возросла производительность используемых компьютеров.

Поэтому квалифицированный криптограф должен быть очень осторожным и осмотрительным, когда работает с длинным открытым ключом. Необходимо учитывать, насколько ценна засекречиваемая с его помощью информация и как долго она должна оставаться в тайне для посторонних.

А почему не взять 10 000-битный ключ? Ведь тогда отпадут все вопросы, связанные со стойкостью несимметричного алгоритма шифрования с открытым ключом, основанном на разложении большого числа на множители. Но дело в том, что обеспечение достаточной стойкости шифра — не единственная забота криптографа. Имеются дополнительные соображения, влияющие на выбор длины ключа, и среди них — вопросы, связанные с практической реализуемостью алгоритма шифрования при выбранной длине ключа.

Чтобы оценить длину открытого ключа, будем измерять доступную криптоаналитику вычислительную мощь в так называемых мопс-годах, т. е. количеством операций, которые компьютер, способный работать со скоростью 1 млн операций в секунду, выполняет за год. Допустим, что злоумышленник имеет доступ к компьютерным ресурсам общей вычислительной мощностью 1000 мопс-лет, крупная корпорация — 107 мопс-лет, правительство — 109 мопс-лет. Это вполне реальные цифры, если учесть, что при реализации упомянутого выше проекта разложения числа из 129 цифр его участники задействовали всего 0,03% вычислительной мощи Internet, и чтобы добиться этого, им не потребовалось принимать какие-либо экстраординарные меры или выходить за рамки закона. Из табл. 4.6 видно, сколько требуется времени для разложения различных по длине чисел.

Сделанные предположения позволяют оценить длину стойкого открытого ключа в зависимости от срока, в течение которого необходимо хранить зашифрованные с его помощью данные в секрете (табл. 4.7). При этом нужно помнить, что криптографические алгоритмы с открытым ключом часто применяются для защиты очень ценной информации на весьма долгий период времени. Например, в системах электронных пла-

Таблица 4.6. Связь длины чисел и времени, необходимого для их разложения на множители

Количество бит в двоичном представлении числа	Количество мопс-лет для разложения на множители
768	3×10^5
1024	3×10^7
1280	3×10^9
1536	3×10^{11}
2048	3×10^{14}

тежей или при нотариальном заверении электронной подписи. Идея потратить несколько месяцев на разложение большого числа на множители может показаться кому-то очень привлекательной, если в результате он получит возможность рассчитываться за свои покупки по чужой кредитной карточке.

Таблица 4.7. Рекомендуемая длина открытого ключа (в битах)

Год	Хакер	Крупная корпорация	Правительство
2000	1024	1280	1536
2005	1280	1536	2048
2010	1280	1536	2048
2015	1536	2048	2048

С приведенными в табл. 4.7 данными согласны далеко не все криптографы. Некоторые из них наотрез отказываются делать какие-либо долгосрочные прогнозы, считая это бесполезным делом, другие — чересчур оптимистичны, рекомендуя для систем цифровой подписи длину открытого ключа всего 512—1024 бита, что является совершенно недостаточным для обеспечения надлежащей долговременной защиты.

Криптоаналитическая атака против алгоритма шифрования обычно бывает направлена в самое уязвимое место этого алгоритма. Для организации шифрованной связи часто используются криптографические алгоритмы как с секретным, так и с открытым ключом. Такая криптосистема называется гибридной. Стойкость каждого из алгоритмов, входящих в состав гибридной криптосистемы, должна быть достаточной, чтобы успешно противостоять вскрытию. Например, глупо применять симметричный алгоритм с ключом длиной 128 бит совместно с несимметричным алгоритмом, в котором длина ключа составляет всего 386 бит. И наоборот, не имеет смысла задействовать симметричный алгоритм с ключом длиной 56 бит вместе с несимметричным алгоритмом с ключом длиной 1024 бита.

Таблица 4.8. Длины ключей для симметричного и несимметричного алгоритмов шифрования, обладающих одинаковой стойкостью

Длина ключа, бит	
Для симметричного алгоритма	Для несимметричного алгоритма
56	384
64	512
80	768
112	1792
128	2304

В табл. 4.8 перечисляются пары длин ключей для симметричного и несимметричного криптографического алгоритма, при которых стойкость обоих алгоритмов против криптоаналитической атаки методом тотального перебора приблизительно одинакова. Из этих данных следует, что если используется симметричный алгоритм с 112-битным ключом, то вместе с ним должен применяться несимметричный алгоритм с 1792-битным ключом. Однако на практике ключ для несимметричного алгоритма шифрования обычно выбирают более стойким, чем для симметричного, поскольку с помощью первого защищаются значительно большие объемы информации и на более продолжительный срок.

Способы генерации ключей

Поскольку стойкость шифра определяется секретностью ключа, то вскрытию может подвергнуться не сам шифр, а алгоритм генерации ключей. Иными словами, если для генерации ключей используется нестойкий алгоритм, криптосистема будет нестойкой.

Длина ключа в DES-алгоритме составляет 56 бит. Вообще говоря, в качестве ключа можно использовать любой 56-битный вектор. На практике это правило часто не соблюдается. Например, широко распространенная программа шифрования файлов Norton Discreet, входящая в пакет Norton Utilities (версии 8.0 или более младшей версии), которая предназначена для работы в операционной системе DOS, предлагает пользователю программную реализацию DES-алгоритма. Однако при вводе ключа разрешается подавать на вход программы только те символы, старший бит представления которых в коде ASCII равен нулю. Более того, пятый бит в каждом байте введенного ключа является отрицанием шестого бита, и в нем игнорируется младший бит. Это означает, что мощность ключевого пространства сокращается до 240 ключей. Таким образом, программа Norton Discreet реализует алгоритм шифрования, ослабленный в десятки тысяч раз по сравнению с настоящим DES-алгоритмом.

В табл. 4.9 приведено количество возможных ключей в зависимости от различных ограничений на символы, которые могут входить в ключевую последовательность, а также указано время, необходимое для проведения атаки методом тотального перебора, при условии, что перебор ведется со скоростью 1 млн ключей в секунду.

Из табл. 4.9 следует, что при переборе 1 млн ключей в секунду можно в приемлемые сроки вскрывать 8-байтовые ключи из строчных букв и цифр, 7-байтовые буквенно-цифровые ключи, 6-байтовые ключи, составленные из печатаемых ASCII-символов, и 5-байтовые ключи, в которые могут входить любые ASCII-символы. А если учесть, что вычислительная мощность компьютеров увеличивается вдвое за 1,5 года, то для успешного отражения атаки методом тотального перебора в течение ближайшего десятилетия необходимо заблаговременно позаботиться о том, чтобы используемый ключ был достаточно длинным.

Когда отправитель сам выбирает ключ, с помощью которого он шифрует свои сообщения, его выбор обычно оставляет желать лучшего. Например, некий Петр Сергеевич Иванов скорее предпочтет использовать в качестве ключа Ivanov, чем такую последовательность символов, как &!ъ7)g*. И вовсе не потому, что он принципиально не желает соблюдать элементарные правила безопасности. Просто свою фамилию Ива-

Таблица 4.9. Количество возможных ключей в зависимости от ограничений на символы ключевой последовательности

Используемые символы	Длина символов ключевой последовательности, байт									
	4		5		6		7		8	
	Количество возможных ключей	Время полного перебора	Количество возможных ключей	Время полного перебора	Количество возможных ключей	Время полного перебора	Количество возможных ключей	Время полного перебора	Количество возможных ключей	Время полного перебора
Строчные буквы (26)	$4{,}7x10^5$	0,6 с	$1{,}3x10^7$	13с	$3{,}2x10^8$	6 мин	$8{,}1x10^9$	2,3 час	$2{,}2x10^{11}$	2,5 дн
Строчные буквы и цифры (36)	$1{,}8x10^6$	1,8 с	$6{,}1x10^7$	2 мин	$2{,}3x10^9$	37 мин	$7{,}9x10^{10}$	23 час	$2.9x10^{12}$	34 дн.
Буквы и цифры (62)	$1{,}6x10^7$	16с	$9{,}3x10^8$	16 мин	$5{,}8x10^{10}$	17 час	3,6x10"	42 дн.	2,3x10"	7,0 лет
Печатаемые символы (95)	$8{,}2x10^7$	1,5 мин	$7{,}8x10^9$	2,2 час	$7{,}5x10^{11}$	8,6 дн.	$7{,}1x10^{13}$	2,3 лет	$6{,}7x10^{15}$	211 лет
Все ASCII-символы	$4{,}4x10^9$	1,3 час	$1{,}2x10^{10}$	14дн.	$2{,}9x10^{14}$	9,0 лет	$7{,}3x10^{16}$	2400 лет	$1{,}9x10^{19}$	590000 лет

нов помнит гораздо лучше, чем абракадабру из восьми произвольно взятых символов. Однако при использовании такого ключа сохранить свою переписку в тайне ему не поможет и самый стойкий алгоритм шифрования в мире, особенно если ключи совпадают с именами ближайших родственников и записывает он эти ключи на клочках бумаги, которые наклеивает на компьютер. В ходе хорошо организованной атаки методом тотального перебора квалифицированный криптоаналитик не будет применять все ключи последовательно, один за другим. Он сначала проверит те из них, которые хоть что-то значат для Иванова. Такая разновидность атаки методом тотального перебора называется словарной атакой, поскольку противник использует словарь наиболее вероятных ключей. В этот словарь обычно входят:

- Имя, фамилия, отчество, инициалы, год рождения и другая личная информация, имеющая отношение к данному человеку. Например, при словарной атаке против Петра Сергеевича Иванова в первую очередь следует проверить PSI. PSIPSI, PIVANOV, Pivanov, psivanov, peteri, petel, IvanovP, peterivanov, Peter-Ivanov и т. д.
- Словарная база данных, составленная из имен людей, героев мультфильмов и мифических животных, ругательств, чисел (как цифрами, так и прописью), названий художественных фильмов, научно-фантастических романов, астероидов, планет и цветов радуги, общепринятых сокращений и т. д. В общей сложности для одного конкретного человека такая база данных насчитывает более 60 тыс. словарных единиц.
- Слова, которые получены путем внесения различных изменений в словарную базу данных, составленную на предыдущем этапе. Сюда относятся обратный порядок написания слова, замена в нем латинских букв o, 1, z, s на цифры 0, 1, 2 и 5 соответственно, слова во множественном числе и т. д. Это дает дополнительно еще около миллиона словарных единиц для использования в качестве возможного ключа к шифру.
- Слова, полученные с помощью замены строчных букв на заглавные. Например, вместе со словом Ivanov будут проверяться слова iVanov, ivAnov, ivaNov, ivanOv, ivanoV, IVanov, IvAnov, IvaNov, IvanOv, IvanoV и т. д. Однако вычислительная

мощь современных компьютеров позволяет проверять только одно-, двух- и трехбуквенные замены строчных букв на заглавные.

- Слова на различных иностранных языках. Хотя компьютерные пользователи, в основном, работают с англоязычными операционными системами (DOS, UNIX, Windows и др.), существуют локализованные версии распространенных операционных систем, в которых допускается использование другого языка. Это означает, что в качестве ключа на вход программы шифрования может быть подана любая фраза на родном языке ее пользователя. Следует также учитывать, что ключ может быть транслитерирован с любого языка (например, с/русского или китайского) на английский и затем в таком виде введен в программу шифрования.
- Пары слов. Поскольку количество вероятных пар слов, из которых может состоять криптографический ключ, слишком велико, на практике криптоаналитики обычно ограничиваются словами из трех и четырех букв.

Поэтому, если все же требуется сохранить ключ в памяти, а запомнить выражение (например, 36f9 67a3 f9cb d931) трудно, тогда для генерации ключа можно использовать правила, которые очевидны для вас, но не для постороннего:

- Составьте ключ из нескольких слов, разделенных знаками препинания. Например, легко запоминаются ключи типа Yankee! Go home.
- Используйте в качестве ключа сочетание букв, которые представляют собой акроним более длинного слова. К примеру, отбросив гласные буквы в предыдущем выражении, можно сгенерировать ключ Ynk! G hm.

Более привлекателен подход, при котором вместо отдельного слова используется достаточно длинное, легко запоминающееся предложение на русском, английском или другом языке. Такое выражение в криптографии называется паролем. Для преобразования пароля в псевдослучайный битовый ключ можно применить любую однонаправленную хэш-функцию.

Пароль следует выбирать достаточно длинным, чтобы полученный в результате его преобразования ключ был случайным. Известно, что в предложении на английском языке каждая буква содержит примерно 1,3 бита информации. Тогда, чтобы получить 64-битный ключ, пароль должен состоять примерно из 49 букв, что соответствует английской фразе из 10 слов.

Пароль должен быть составлен так, чтобы его было легко вспоминать, и в то же время он должен быть достаточно уникальным. Цитата из высказываний Козьмы Пруткова, которая у всех на слуху, вряд ли подойдет, поскольку его сочинения имеются в форме, доступной для воспроизведения на компьютере, и, следовательно, могут быть использованы в словарной атаке. Лучше воспользоваться творчеством малоизвестного поэта или драматурга, процитировав его с ошибками. Эффект будет сильнее, если в цитате, использованной для генерации ключа, присутствуют иностранные слова. Идеально подходят для этой цели незатейливые ругательства — их не придется записывать, чтобы запомнить. Достаточно стукнуть по пальцу молотком, и пароль автоматически придет вам в голову. Надо только сдержаться и не произнести его вслух, чтобы не подслушали посторонние.

Несмотря на все сказанное, залогом наилучшей защиты служит не шаманство при выборе пароля, а случайность полученного ключа. Хороший ключ — это случайный ключ, а значит, заранее будьте готовы к тому, что запомнить его наизусть очень труд-

но. Поскольку в компьютерах используется исключительно цифровая информация, то далее мы будем предполагать, что сообщение, которое мы хотим криптографически преобразовать, переводится в последовательность двоичных цифр. Любая информация (письма, музыка или телевизионный сигнал) может быть представлена в двоичном коде.

Надежный ключ представляет собой случайный битовый вектор. К примеру, если он имеет длину 56 бит, это значит, что в процессе его генерации с одинаковой вероятностью может получиться любой из 256 возможных ключей. Источником случайных ключей обычно служит природный случайный генератор. Кроме того, источником случайного ключа может быть криптографически надежный генератор псевдослучайных двоичных последовательностей. Лучше, чтобы процесс генерации ключей был автоматизирован.

Использовать хороший генератор случайных чисел является очень важно, однако не следует слишком долго спорить о том, какой из генераторов лучше. Важнее применять стойкие алгоритмы шифрования и надежные процедуры работы с ключами.

Во всех алгоритмах шифрования имеются так называемые нестойкие ключи. Это означает, что некоторые из ключей к шифру менее надежны, чем остальные. Поэтому при генерации ключей нужно автоматически проверять их на стойкость и генерировать новые вместо тех, которые эту проверку не прошли. К примеру, в DES-алгоритме имеются всего 24 нестойких ключа из общего количества 256, и, следовательно, вероятность найти нестойкий ключ пренебрежимо мала. Кроме того, откуда криптоаналитику знать, что для зашифрования конкретного сообщения или файла был применен именно нестойкий ключ? А сознательный отказ от использования нестойких ключей дает противнику дополнительную информацию о вашей криптосистеме, что весьма нежелательно. С другой стороны, проверить ключи на нестойкость достаточно просто, чтобы этим пренебрегать.

Генерировать открытые ключи сложнее, чем секретные, поскольку открытые ключи должны обладать определенными свойствами (например, произведением двух простых чисел).

Рассмотрим подробнее процесс формирования различных ключей. Чтобы усложнить шифр, используется не одна-единственная таблица, с помощью которой можно по некоторому правилу переставить буквы или цифры исходного сообщения, а несколько таблиц в определенном порядке. Этот порядок и образует ключ шифрования. Если мы используем только две таблицы, обозначенные как «ключ 0» и «ключ 1», то типовым ключом может быть, например, 1101101. В связи с тем, что таблиц несколько, теперь мы будем иметь дело с многоалфавитной подстановкой. И таких таблиц теоретически может быть сколь угодно много. Относительно этого нового источника сложности в шифре возникает вопрос: можно ли упростить таблицы подстановок, сделав их меньше? Конечно же, да. Простейшая двоичная подстановка, которую только можно выполнить, — это замена одной двоичной цифры на другую. В этом случае существует всего две различные таблицы подстановок. Рассмотрим их. При этом каждая таблица будет соответствовать одному из двух основных типов ключа, как показано на рис. 4.22.

Мы предположим, что таблица, помеченная «Ключ 1», заменяет нули сообщения на единицы и, наоборот, таблица, помеченная «Ключ 0», оставляет все цифры сообще-

	Сообщение		Шифр	
Ключ 0	0	1	0	1
Ключ 1	0	1	1	0

Рис. 4.22. Двоичная подстановка

ния неизменными. Оказывается, что тот же самый эффект можно получить с помощью сложения по модулю 2: две одинаковые цифры в результате такой операции дают О, две различные — 1. Поэтому в рассматриваемом случае шаблонный ключ можно назвать также аддитивным ключом. Ключ шифрования для сложения по модулю 2 может быть произвольной последовательностью единиц и нулей. Чтобы зашифровать двоичное представление, прибавляют цифры ключа к каждой цифре сообщения. При расшифровке вычитают цифры (это то же самое, что и сложение по модулю 2),

Рассмотрим, что получится, если мы будем шифровать сообщение (последовательность двоичных цифр), например, 010110, преобразуя ее в другую последовательность, используя ключ «Ключ 1» и «Ключ 0» в некотором произвольном порядке: 110101 (см. рис. 4.22). Согласно правилу, по которому «Ключ 1» заменяет нули сообщения на единицы и наоборот, а «Ключ 0» оставляет все цифры неизменными, получим шифрованное сообщение 100011. Это сложение по модулю 2, удобное тем, что вычитание по модулю 2 есть то же самое, что и сложение, поэтому исходное сообщение может быть восстановлено просто прибавлением последовательности цифр ключа (она известна тому, кому направлено сообщение) к последовательности цифр шифрованного сообщения. Результатом этих преобразований будет расшифрованное сообщение 010110.

Сразу возникает вопрос: имеет ли рассмотренный простой шифр какое-либо практическое значение? Поскольку этот шифр, в сущности, использует лишь две таблицы подстановки минимального размера, очевидно, что мы должны переключаться между ними часто, и делать это случайным образом, то есть прибавлять к данным случайную последовательность ключевых цифр. Предположим, это мы сделали. Тогда получим потенциально нераскрываемый шифр. С точки зрения теории информации этот шифр делает следующее: к каждому биту информации сообщения прибавляется один бит информации (а точнее, дезинформации!) ключа. Этого достаточно, чтобы полностью разрушить любую структуру, которую исходное сообщение могло бы иметь, если только цифры ключа взяты в случайном порядке, скажем, определяемом подбрасыванием монеты, и ключевая последовательность имеет такую же длину, как сообщение, и никогда не повторяется.

Стойкость такого метода определяется исключительно тем, что для каждой цифры сообщения мы полностью и случайным образом меняем ключ. Это единственный класс

шифров, для которых можно доказать нераскрываемость в абсолютном смысле этого слова.

Даже если злоумышленник пытается вскрыть систему с помощью грубой силы, например, опробует все возможные прибавляемые ключи (26 или 64, в случае нашего 6-битного сообщения), он получит все возможные открытые тексты, включая тот, который мы в действительности зашифровали, но не получит информации о том, какое сообщение правильное. Даже сам дьявол, который мог бы опробовать все возможные ключи в одно мгновение, не мог бы внести определенность. Эта система хорошо известна и используется всеми правительствами под разными именами, такими, как система Вернама или одноразовый блокнот.

В реальных системах требуется, чтобы на передающей и приемной сторонах были одинаковые ключи, синхронизированные посредством таймера. Цифры сообщения и цифры ключа складываются по модулю 2, полученный в результате зашифрованный поток передается через канал связи, после чего ключ вычитается из данных (прибавляется по модулю 2). Для трафика большого объема обширные запасы ключевых цифр должны быть заблаговременно доставлены получателю и храниться у него.

Фундаментальный недостаток системы Вернама состоит в том, что для каждого бита переданной информации получателю необходимо хранить один заранее подготовленный бит ключевой информации. Более того, эти биты должны следовать в случайной последовательности, и эту последовательность нельзя использовать вторично. Если необходимо шифровать трафик большого объема, то выполнить это требование трудно. Поэтому система Вернама используется только для передачи сообщений наивысшей секретности.

Чтобы обойти проблему предварительной передачи получателю сообщения секретного ключа большого объема, инженеры и изобретатели придумали много остроумных схем генерации очень длинных потоков псевдослучайных цифр из нескольких коротких потоков в соответствии с некоторым алгоритмом. Получателя шифрованного сообщения при этом необходимо снабдить точно таким же генератором, как и у отправителя. Конечно, такой алгоритм предполагает использование систематических процедур, добавляющих регулярности в шифротекст, обнаружение которых может помочь аналитику дешифровать сообщение.

Один из основных методов построения подобных генераторов заключается в использовании двух или более битовых потоков, данные которых побитно складываются для получения единого «смешанного» потока. Например, простой длинный поток битов ключа может быть заменен двумя циклическими генераторами двоичных последовательностей, длины которых являются простыми или взаимно простыми числами (рис. 4.23). Так как в этом случае величины длин двоичных последовательностей не имеют общих множителей, полученный из них поток имеет период повторения, равный произведению их длин.

Например, две двоичные последовательности, имеющие длину 1000 и 1001 двоичных символов соответственно, дают в результате составной псевдослучайный поток, который не повторяется на первых 10001001, или 1001000 цифрах. Циклические двоичные последовательности проходят через сумматор, который складывает по модулю 2 считанные с них цифры. Выход сумматора служит ключом, используемым для зашифрования сообщения. Поэтому важно, чтобы составной поток превышал по длине

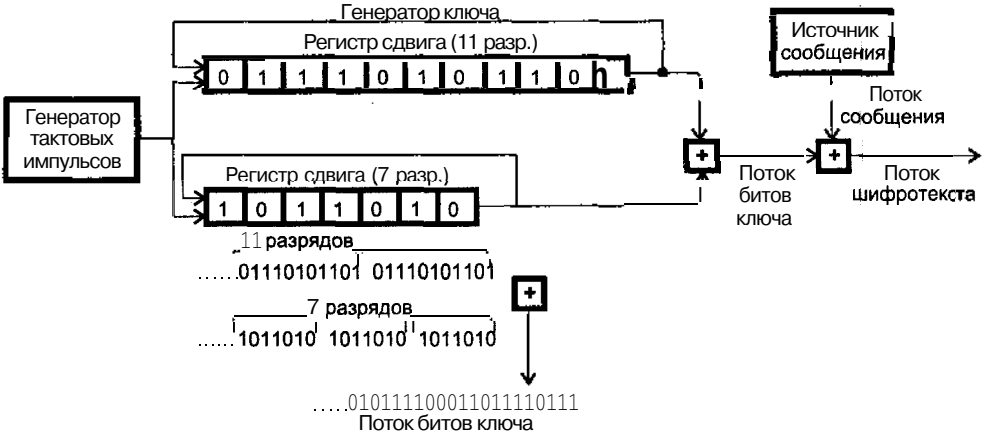


Рис. 4.23. Генератор потокового ключа

все вместе взятые сообщения, которые могут быть переданы за разумный период времени. Расшифрование осуществляется с помощью ключа, сгенерированного на приемнике идентичным способом. Таким образом, несколько коротких последовательностей заменяют одну длинную, но получающиеся при этом внутренние периодичности могут помочь аналитику в раскрытии шифра.

Поскольку побитовый сумматор является линейным устройством, он изначально криптографически слаб, но может быть усилен разными способами. Можно нагромождать одну сложность на другую, вводя цепочки обратной связи, связанные каким-либо образом с передаваемым сообщением, или вводя такие нелинейные математические операции, как подстановки в блоках цифр подходящего размера. Несекретная криптографическая литература содержит много конструкций генераторов псевдослучайных последовательностей, которые могут быть, в принципе, сведены к одной базовой схеме, изображенной на рис. 4.24. Тем или иным способом они вырабатывают псевдослучайные числа, выполняя сложные математические операции над упорядоченной последовательностью входных чисел, преобразуя их способом, который, как предполагается, должен поставить аналитика в тупик.

В этом обобщенном представлении генератора формирования двоичной ключевой последовательности двоичный счетчик обеспечивает входными числами блок преобразований, который вырабатывает биты потока ключа, прибавляемые затем к потоку битов сообщения в зависимости от состояния селектора ключа.

Но даже шифр Вернама на самом деле не обеспечивает защиту от искусного мошенничества с трафиком, не обладающим избыточностью.

Независимо от того, закодировано ли сообщение с использованием случайных цифр или псевдослучайной последовательности цифр, в подобном побитовом шифровании одиночная ошибка, возникшая при передаче сообщения, остается в рамках одной цифровой позиции; ошибка не «размножается» и не распространяется на остаток сообщения. Кроме того, этот шифр не вносит межсимвольных зависимостей. Когда сообщение написано на естественном языке, то контекст естественной избыточности позволяет человеку, читающему текст, легко обнаруживать случайные ошибки. Так, если неко-

торые из 5 бит, представляющих букву Е, оказались искаженными таким образом, что соответствующая группа битов стала представлением буквы О (например, слово СЕКРЕТНЫЙ превратилось в слово СЕКРОТНЫЙ), то читатель-человек, исходя из контекста, обнаружил бы ошибку.

Совершенно иная ситуация при использовании компьютеров. Передаваемые данные здесь могут не содержать избыточности, например, если они полностью числовые, то в этой ситуации ошибка всего в одной цифре может вызвать целый каскад вычислительных погрешностей. Изучение проблемы показало, что простые коды обнаружения ошибок не подходят для защиты целостности компьютерных данных от возможных подтасовок со стороны злоумышленников. В данном случае необходимо не просто обнаружение ошибок, а требуется аутентификация, защищенная криптографическими методами. Неожиданно оказалось, что это лучше всего достигается, если решение строить на принципах, внутренне присущих шифрующим структурам.

Наибольшая производительность компьютеров достигается при их работе с блоками данных длиной 8, 16, 32 и т. д. разрядов. Рассмотрим порядок формирования ключей для блочных шифров. Блочным шифром будем называть любой шифр, который преобразует п цифр сообщения в п цифр шифрограммы.

Например, блочным будет такой шифр, который преобразует код 00000, представляющий по нашему соглашению букву А в открытом тексте, в, скажем, 11001, эквивалент А для шифротекста, по некоторому ключу перестановки, в точности, как это задает таблица подстановок. Чтобы увидеть, как такое двоичное преобразование выполняется электронным устройством, давайте рассматривать подстановки только в группах из трех двоичных цифр, как это показано на рис. 4.25.

Блок подстановок, в отличие от потоковых устройств, включает как линейные, так и нелинейные преобразования: он не просто прибавляет нули и единицы к цифрам входа, но может заменить любой входной блок цифр на любой выходной блок. Реально он состоит из двух коммутаторов. Первый преобразует двоичное число из п цифр в одну цифру по основанию 2п, другой выполняет обратное преобразование. Блок, таким образом, содержит 2п внутренних соединений коммутаторов, которые могут быть выполнены 2п! различными способами. Это означает, что в случае изображенного на рис. 4.25 блока с п = 3 существует 23! = 8! = 40320 различных вариантов разводки блока или таблиц, подобных той, что изображена на этом рисунке. Блок такого типа с п = 128 сделал бы криптоанализ практически неосуществимым, однако его трудно создать технологически.

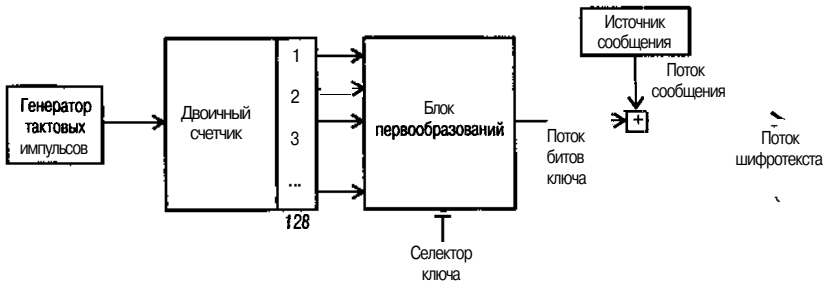
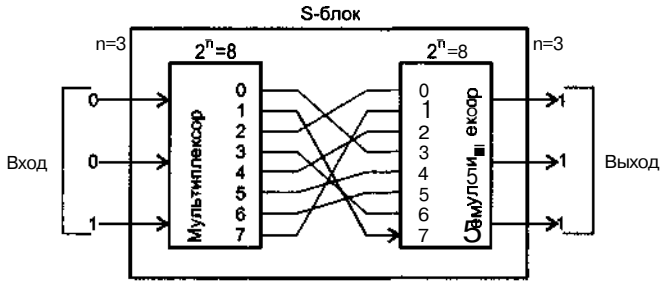


Рис. 4.24. Схема формирования двоичной ключевой последовательности



Вход	Выход
001	011
001	111
010	000
011	110
100	010
101	100
110	101
111	001

Рис. 4.25. Порядок работы блока подстановок

Рассмотрим, как работает блок подстановок в нашем случае. С помощью трех двоичных цифр можно представить восемь элементов: 23 = 8. Устройство, выполняющее подстановку, как мы видим, состоит из двух коммутаторов. Первый (мультиплексор) преобразует последовательность из трех двоичных цифр в соответствующее восьмеричное значение, подавая сигнал на одну из восьми выходных линий (в нашем случае это линия 1). Эти 8 выходов могут быть соединены с восемью входами второго переключателя любым из 8! (или 40320) способов. Из этого множества различных вариантов соединения или коммутации проводов между первым и вторым переключателем мы можем выбрать тот, который будем использовать. Задача второго переключателя (демультиплексора) — преобразовать входной сигнал, представленный одной цифрой по основанию 8, обратно в трехразрядный двоичных выход.

Если бы устройство подстановки было построено для обработки пятицифрового двоичного входа, его можно было бы использовать для зашифрования алфавита из 32-х символов. Возможных соединений двух переключателей было бы тогда 32!. Может показаться, что ключей очень много, но к созданному таким образом шифру все же необходимо относиться, как к очень слабому: он поддается частотному анализу. Эта слабость не является его неотъемлемым свойством. Рассмотренное устройство с математической точки зрения определяет наиболее общее возможное преобразование. Оно включает для любого заданного размера входа-выхода любой возможный обратимый шифр, который когда-либо был, или даже просто мог бы быть изобретен; математики могли бы сказать, что он представляет полную симметричную группу. Он полностью «несистематический»: одно соединение переключателей ничего не говорит злоумышленнику относительно всех других соединений. Слабость данного шифра обусловлена выбранным размером блока. Несмотря на большое количество ключей, каталог возможных входов и выходов очень мал: в нем всего лишь 32 элемента. Нам же необходим такой большой каталог, чтобы для любого злоумышленника было практически невозможно записать его. Если взять, например, блок со 128 входами и выходами, то аналитику было бы необходимо рассмотреть 2128 (или больше 1038) возможных блоков цифр. Это настолько огромное число, что частотный анализ здесь просто неосуществим. К несчастью, устройство подстановок со 128 входами также потребовало бы 2128 внутренних соединений между первым и вторым переключателями, что технологически очень сложно реализуется.

Однако существует преобразование, которое легко реализовать для большого набора входов. Практически выполнимо, например, построить блок со 128 входными и

выходными выводами, которые внутри соединены обычными проводами, как показано на рис. 4.26.

Для такого «блока перестановок» с n выходами имеется n! возможных вариантов коммутации проводов, каждый из которых определяется отдельным ключом. Он легко может быть построен для n = 128. И хотя это обеспечит большое количество возможных ключей (128!), что весьма полезно, мы теперь столкнемся с новой трудностью. Путем использования набора специально сконструированных сообщений можно целиком определить ключ такой системы всего за n-1 попыток (в данном случае 127). Этот прием состоит в том, чтобы использовать серию сообщений, содержащих одну-единственную единицу в n-1 различных позициях. Позиция единицы в выходном блоке определит использованное в устройстве подключение провода. Слабость простого блока перестановок заключается в том, что он является линейной системой.

Для повышения стойкости используемого шифра необходим некоторый компромиссный вариант, который бы, как минимум, приближался по характеристикам к общей системе. Это возможно сделать, используя составной шифр, в котором два или более шифра скомбинированы так, что результирующая система обладает большей стойкостью, чем каждая из составляющих ее систем в отдельности. Перед первой мировой войной были исследованы громоздкие шифры, включающие несколько этапов шифрования. Первым действительно успешным образцом была, вероятно, система, изобретенная немцами, известная как ADFCVX-система. Она соединяла «дробления» с «перестановками». Иными словами, в этой процедуре сообщение разбивалось на сегменты и сегменты переставлялись на другие места. Важный факт, на который следует обратить внимание, заключается в том, что шифр, составленный из блочных шифров, опять является блочным шифром. Цель в том, чтобы шифр вел себя подобно общему шифру замен настолько, насколько это возможно.

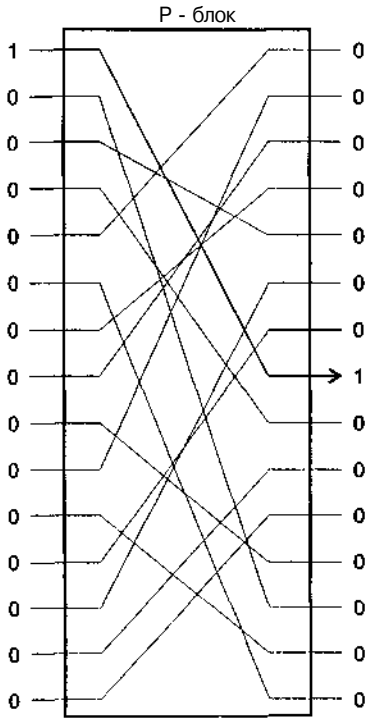


Рис 4.26. Блок перестановок с большим количеством вариантов коммутации

Между первой и второй мировыми войнами интерес к составным шифрам практически полностью пропал благодаря успешному развитию роторных или проводно-дисковых машин, которые принадлежат к общему классу генераторов псевдослучайных последовательностей. Типичная роторная машина имела клавиатуру, напоминающую клавиатуру пишущей машинки. Каждая буква шифровалась с помощью нескольких дисков, работающих в определенной последовательности, для очередной шифруемой буквы диски переводились в другое положение с использованием нерегулярного алгоритма, зависящего от ключа. Сообщение расшифровывалось идентичной машиной с точно таким же установленным ключом.

Сейчас интерес к составным шифрам возник благодаря статье «Теория связи в секретных системах» Клода Шеннона, которая была опубликована в техническом журнале корпорации Bell (Bell System Technical Journal) в 1949 году. В разделе, посвященном практической разработке шифров, Шеннон ввел в рассмотрение понятия «перемешивания» и «рассеивания», а также понятие «перемешивающего преобразования», которое предполагает особый способ использования результатов преобразования. Его статья открыла практически неограниченные возможности по разработке и исследованию шифров.

Способ, которым следует сочетать принципы перемешивания и рассеивания для получения криптографической стойкости, можно описать следующим образом: перестановки общего вида не могут быть реализованы для больших значений n, скажем, для n = 128, и поэтому мы должны ограничиться схемами подстановки, имеющими практический размер. Например, в системе «Люцифер» для блоков подстановки выбрано n = 4. Хотя это число может показаться слишком маленьким, такая подстановка может оказаться вполне эффективной, если ключ подстановки или схема коммутации проводников выбраны верно. В системе «Люцифер» нелинейная подстановка эффективно обеспечивает определенную степень перемешивания.

В этой системе входные данные пропускаются через чередующиеся уровни блоков, которые обозначены на предыдущих рисунках символами P и S. В блоке перестановок P n — большое число (128 или 64), а в блоке подстановок S число n мало (4). Несмотря на то, что P- и S-блоки в отдельности составили бы слабую систему, в комбинации друг с другом они устойчивы.

Проиллюстрируем меру стойкости подобных конструкций на примере устройства (составной шифрующей системы), изображенного на рис. 4.27, в котором для простоты P-блоки имеют размер n = 15, а S-блоки — n = 3. Если изобразить этот «бутерброд» из блоков со специально сконструированным входным числом, составленным из 14 нулей и одной-единственной единицы, то легко будет увидеть перемешивание и рассеивание в работе. Первый блок P передает единственную единицу на вход некоторого блока S, который, будучи нелинейным устройством, может преобразовать единицу в трехцифровой выход, содержащий в потенциале целых 3 единицы. В показанном на диаграмме варианте он вырабатывает две единицы. Следующий блок P тасует две единицы и передает их на вход двух различных S-блоков, которые вместе имеют потенциал по выработке уже шести единиц. Дальше диаграмма говорит сама за себя: по мере того, как входной блок данных проходит через последовательные уровни, узор из сгенерированных единиц расширяется и дает в результате непредсказуемый каскад цифр. Конечный результат, получающийся на выходе всей цепочки, будет содержать в среднем половину нулей и половину единиц, в зависимости от ключей перестановки, использованных в различных P- и S-блоках.

Очень важно, что все выходные цифры потенциально стали сложными функциями всех входных цифр. Поскольку все блоки имеют независимые ключи, поток вырабатываемых цифр и окончательный результат не могут быть предсказаны. Цель разработчика, конечно, — сделать предельно трудным для злоумышленников прослеживание цепочки назад и, таким образом, реконструировать ключи в P- и S-блоках.

В реальной системе S-блок, например, являясь достаточно общим преобразованием, может случайно быть снабжен таким ключом, что поведет себя в точности как P-

блок, и в этом случае вся система будет не более стойкой, чем один слой P, который может быть достаточно просто раскрыт. Чтобы этого избежать, блоки обоих типов снабжают постоянными ключами, которые должны быть сильными; эти постоянные ключи будут известны каждому, кто имеет доступ к системе. Следовательно, необходим другой способ использования ключей, при этом желательно, чтобы они могли быть представлены двоичными числами. Этого можно достигнуть, построив «бутерброд», в котором каждый S-блок содержит два различных постоянных ключа, и, таким образом, может быть представлен двумя возможными различными состояниями — SO и S1. Последовательность этих состояний для любого отдельного «бутерброда» составляет управляемую ключом структуру, не известную потенциальному противнику. Эту структуру можно представить двоичным ключом, который указывает, которую из двух таблиц подстановки следует использовать, в точности как в случае двухтабличной подстановки, рассмотренной выше. Цифры ключа можно загрузить в ключевой регистр криптографического устройства и записать на ключевую магнитную карту, закрепленную за законным пользователем системы. Когда два состояния S-блоков используются подобным образом, результирующая криптограмма показывает межсимвольные зависимости, которые делают все цифры выхода сложными функциями не только всех цифр входа, но и всех цифр ключа. Таким образом, эта система устойчива к попыткам проникновения в нее с помощью математических методов анализа.

Хотя межсимвольная зависимость — необходимый (но не достаточный) показатель криптографической стойкости, она имеет и оборотную сторону: влечет за собой чувствительность системы к шуму или помехам во время передачи. Погрешность в

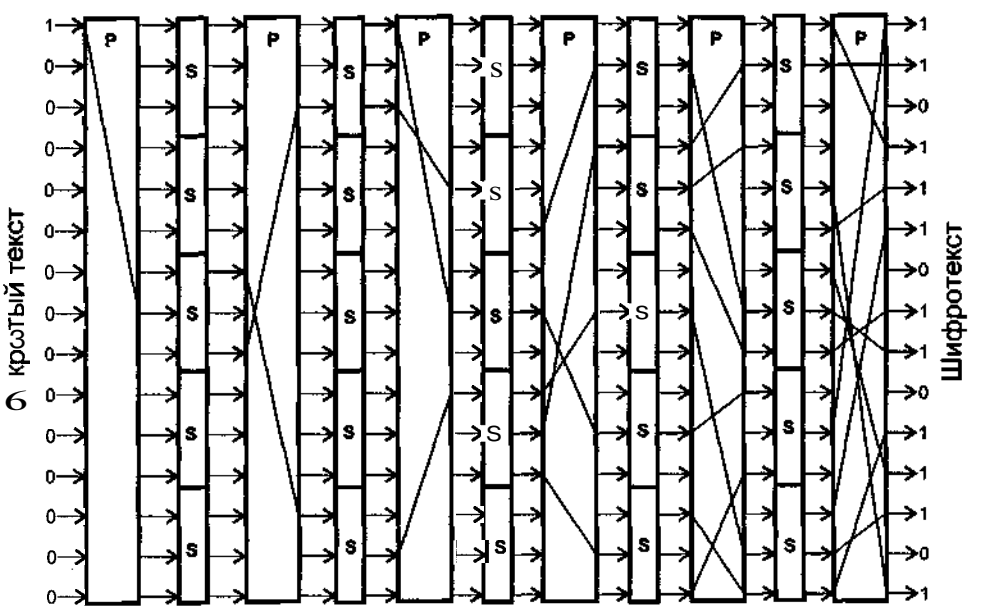


Рис. 4.27. Составная шифрующая система

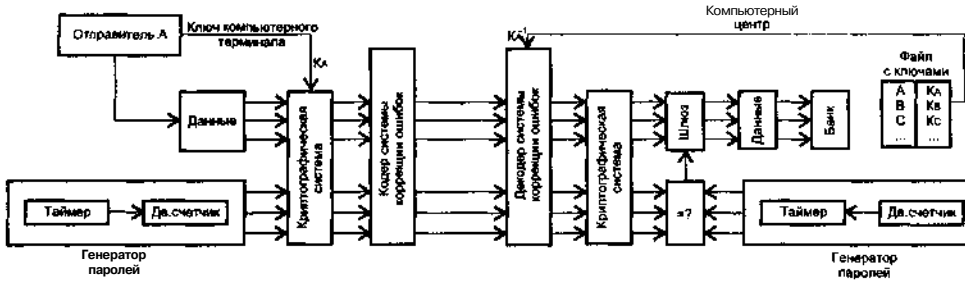


Рис. 4.28. Полная криптографическая система с генератором паролей

единственной цифре может привести к полному искажению расшифрованных данных. Современные средства коммуникации делают, однако, эту проблему менее актуальной, по крайней мере, для невоенного использования.

Более того, сильные взаимозависимости между цифрами могут принести удивительную и неожиданную пользу: поскольку система так чувствительна к изменениям и так резко реагирует на них, она автоматически становится идеальным средством обнаружения изменений, произошедших как случайно, так и сделанных умышленно. В результате получаем одновременно высокую секретность сообщений и неподдающийся обману сигнализатор ошибок.

Чтобы извлечь пользу из этой дополнительной особенности шифра, необходимо всего лишь зарезервировать место для пароля внутри заданного блока цифр сообщения. Пароль — это последовательность цифр, автоматически вводимая в поток цифр сообщения передающей аппаратурой без какого-либо участия лица, использующего систему. Роль пароля заключается в том, чтобы сообщить приемной аппаратуре, что сообщение не было преднамеренно искажено или серьезно испорчено шумом в процессе передачи. Процесс зашифрования оставляет противника в неведении, как биты сообщения и пароля отображены в криптограмме. Если цифры пароля не могут быть без ошибок восстановлены декодером на принимающем конце, сообщение отвергается.

Решающую роль в этой схеме играет генератор пароля, который должен быть как на приемнике, так и на передатчике, как показано на рис. 4.28. Генератор пароля на самом деле является не чем иным, как двоичным таймером или счетчиком, определяющим время или порядковый номер сообщения в двоичной записи, и добавляющим эту группу цифр к каждому блоку цифр передаваемого сообщения. Необходимо учесть, что в определенный момент времени, скажем в 8:00, таймеры на обоих концах канала передачи должны быть синхронизированы и иметь одинаковые частоты.

Полная система объединяет генератор пароля, криптографическую систему, состоящую из S- и P-блоков и систему коррекции ошибок. Генератор паролей вырабатывает новый парольный блок для каждого блока данных. Отправитель, используя персональный ключ, вводит свои данные. Цифры пароля и данных станут не отслеживаемыми после того, как будут зашифрованы в соответствии с ключом. Дополнительные цифры кода коррекции ошибок добавляются к данным перед передачей и изымаются сразу после приема. Криптографическая система компьютерного центра расшифровывает передачу в соответствии с инвертированным ключом отправителя,

который выбирается из специального защищенного файла, хранимого в центре, и извлекает цифры пароля. Если они совпадут с цифрами пароля, сгенерированного в компьютере, шлюз открывается и входные данные передаются в хранилище.

А как же «парольная схема аутентификации» обеспечивает безопасность работы членам сообщества пользователей централизованного хранилища данных, которые имеют доступ к большому центральному компьютеру? Рассмотрим и этот вариант. Каждый пользователь имеет свой собственный секретный ключ, возможно, представленный в форме последовательности двоичных цифр, записанной, например, на магнитную карту или смарт-карту. Ключи всех пользователей хранятся в защищенной форме в центральном компьютере. Предположим, что пользователь с ключом KA хочет передать сообщение на центральный компьютер. Он вставляет карточку, на которой записан его ключ, в считывающий терминал, располагающийся на его рабочем столе, секунду или две ждет сигнала, что линия свободна, и начинает набирать свое сообщение.

Сообщение автоматически разделяется на блоки цифр (скажем, по 64 цифры), которые на каждом сигнале двоичного таймера объединяются с паролем (который также может иметь 64 цифры), соответствующим выходу таймера в этот момент времени. Результирующий блок из 128 цифр шифруется, для чего пропускается через криптосистему P- и S- блоков, которая полностью перемешивает цифры пароля и цифры данных.

Поскольку результирующая криптограмма очень чувствительна к ошибкам передачи, она усиливается с помощью кода исправления ошибок, который реагирует на шум в используемых линиях связи. Добавление этого кода удлиняет блок, содержащий цифры пароля и сообщения, еще на несколько цифр.

Результирующий блок шифрограммы дополняется адресом отправителя в открытом виде и передается на центральный компьютер. Когда сообщение доходит до адресата, ключ KA, принадлежащий пользователю A, отыскивается в соответствующем списке и его обращение загружается в декодер для того, чтобы расшифровать криптограмму.

Будет ли совпадать пароль из полученной криптограммы с паролем, локально выработанным двоичным таймером на принимающей стороне? При отсутствии искажений, и если криптограмма была действительно зашифрована на ключе пользователя A, выход декодера будет состоять из блока цифр данных и блока цифр правильного пароля. Это считается достаточным свидетельством в пользу того, что криптограмма действительно создана пользователем A и система принимает данные.

Что же случится, если произошло искажение данных? Если оно было вызвано шумовыми всплесками в линии связи, то код исправления ошибок устранит его и сообщение успешно пройдет аутентификацию. Если же искажения не могут быть устранены кодом коррекции ошибок, то даже одна неверно принятая цифра произведет эффект лавины в декодирующем устройстве и превратит всю принятую информацию в мусор. Пароли больше не будут совпадать. Система воспримет сообщение, как имеющее подозрительное происхождение, и отвергнет его.

Решающим шагом является проверка того, что парольный тест сработал бы так же надежно, если кто-либо записал бы перехваченное сообщение и повторно передал его позже, когда пароль перестал быть действительным. Конечно, использование неверного ключа — причина для немедленной отбраковки сообщения. Представляется, что

предложенная система устойчива к любой мыслимой попытке обмануть ее. Каждая двоичная цифра пароля обеспечивает один бит аутентифицирующей информации. Если пароль состоит из п цифр, то злоумышленник имеет лишь один шанс из 2n (или один шанс из 264, если п = 64) сгенерировать любым способом такую криптограмму, которая при расшифровке случайно даст истинный пароль. Число 264 равно примерно 1019. Невозможно аутентифицировать данные более эффективно.

Хранение и обновление ключей

Прогресс в области вычислительной техники идет очень быстрыми темпами. Сейчас даже персональные компьютеры повсеместно работают под управлением многозадачных операционных систем. В результате пользователь часто оказывается не в состоянии определить, когда операционная система прерывает выполнение его программы шифрования, записывает ее саму, а также все ее данные на диск и переключается на работу с другим приложением. После того как операционная система возобновляет процесс шифрования, все выглядит вполне пристойно: пользователь даже не успевает осознать, что шифровальная программа вместе с используемым ею ключом побывала на диске. В итоге ключ так и останется на диске в незашифрованном виде, пока поверх него не будут записаны другие данные. Когда это случится — через полсекунды, через месяц или вообще никогда, не может сказать никто. Однако враг не дремлет, и вполне может произойти так, что ключ еще хранится на диске в открытом виде, когда злоумышленник проверит этот диск в поисках полезной для себя информации.

В некоторых случаях для организации обмена шифрованными сообщениями применяются сеансовые ключи. Они называются так потому, что используются лишь в одном сеансе связи, а затем уничтожаются. В результате вероятность их компрометации уменьшается. Еще больше понизить эту вероятность можно с помощью следующего метода.

К сгенерированному ключу (назовем его основным) добавляется битовый управляющий код, который содержит информацию об ограничениях, накладываемых на использование этого ключа. Управляющий код подвергается хэшированию и затем складывается с основным ключом по модулю 2. Полученный результат служит в качестве ключа для зашифрования сеансового ключа. Зашифрованный сеансовый ключ хранится вместе с управляющим кодом. Чтобы получить сеансовый ключ в исходном виде, надо применить хэширование к управляющему коду, сложить его с основным ключом по модулю 2 и использовать результат для расшифрования сеансового ключа. Достоинством этого метода является возможность задействовать управляющий код произвольной длины и открыто хранить его вместе с зашифрованным основным ключом.

Иногда при частой смене ключей оказывается очень неудобно каждый раз передавать их абонентам сети для использования при шифровании и расшифровании сообщений. В качестве выхода из этой неудобной ситуации можно предложить генерацию новых ключей из старых, называемую обновлением ключей.

Если два корреспондента владеют общим криптографическим ключом, то, подав его на вход одной и той же однонаправленной функции, они получат одинаковый результат, из которого смогут выбрать необходимое число бит, чтобы составить из них новый ключ. Необходимо только помнить о том, что новый ключ будет обладать такой

же стойкостью, что и старый. Если противник знает старый ключ, он сможет вычислить для этого ключа соответствующее значение однонаправленной функции и получить в свое распоряжение новый ключ.

Проще всего хранить ключи для криптосистемы, у которой имеется единственный пользователь. Пользователь просто запоминает этот ключ и при необходимости вводит его с клавиатуры компьютера по памяти. Однако поскольку сложный случайный ключ запомнить нелегко, для его хранения можно использовать магнитную карточку, или пластиковый ключ с размещенным на нем постоянным запоминающим устройством (так называемый ПЗУ-ключ) или интеллектуальную смарт-карту. Для ввода такого ключа достаточно вставить его физический носитель в специальный считыватель, подключенный к компьютеру. При этом действительное значение вводимого ключа пользователю неизвестно, и, следовательно, он не сможет его разгласить или скомпрометировать. Способ использования ключа определяется управляющим кодом, записанным на физический носитель вместе с этим ключом.

ПЗУ-ключ очень удобен и понятен для многих. Пользователь гораздо лучше осознает, как правильно обращаться с обычным ключом от замка или системы доступа. Придание криптографическому ключу такого же вида, какой имеет ставший нам привычным ключ от замка, позволяет чисто интуитивно избегать многих ошибок, связанных с хранением криптографических ключей.

С целью дальнейшего уменьшения вероятности компрометации ключа его можно разделить на две части. Первую часть следует реализовать в виде ПЗУ-ключа, а вторую — поместить в память компьютера. Тогда потеря носимой части ключа или его половинки, хранимой в памяти компьютера, не приведет к разглашению криптографического ключа в целом. А части ключа при необходимости можно заменять отдельно друг от друга.

Труднозапоминаемые ключи можно хранить на компьютерном диске в зашифрованном виде. Например, открытый ключ, состоящий из многих цифр, лучше зашифровать с помощью DES-алгоритма и запомнить на диске. Более короткий ключ к DES-алгоритму легче вспомнить, когда понадобится расшифровать открытый ключ.

Если ключи генерируются с использованием хорошего датчика псевдослучайных двоичных последовательностей, может оказаться более удобно не хранить сгенерированные ключи, а каждый раз заново их генерировать, задавая соответствующее начальное значение датчика, которое легко запомнить.

Продолжительность использования и уничтожение ключей

Любой ключ должен использоваться в течение ограниченного периода времени по следующим причинам:

- чем дольше ключ находится в действии, тем больше вероятность того, что он будет скомпрометирован;
- при длительном пользовании одним и тем же ключом увеличивается потенциальный ущерб, который может быть нанесен в случае его компрометации;
- ключ, очень долго применявшийся для шифрования информации, становится лакомым кусочком для противника, у которого появляется стимул потратить на

его вскрытие значительные ресурсы, поскольку полученная выгода позволит оправдать понесенные расходы;

- криптоаналитическую атаку на шифр вести тем легче, чем больше перехваченного шифротекста для него накоплено.

Продолжительность использования ключа во многом зависит от криптосистемы. В различных криптосистемах эта продолжительность должна быть разной. Для шифрования речевых сообщений, передаваемых по телефону, имеет смысл менять ключ после каждого разговора. В выделенных каналах связи продолжительность использования ключа определяется ценностью шифруемой информации и скоростью ее передачи. При скорости в 9600 бит/с смену ключа следует производить реже, чем при скорости в несколько гигабит в секунду. Если условия позволяют, такие ключи необходимо менять, по крайней мере, ежедневно.

Не требуют частой смены ключи шифрования ключей. Они используются от случая к случаю, поэтому объем перехваченного противником шифротекста для них невелик. Кроме того, о свойствах соответствующего ему открытого текста противнику заранее ничего не известно, поскольку хороший ключ представляет собой достаточно случайный набор битов. Однако компрометация ключа шифрования ключей влечет за собой гораздо более серьезные потери, чем это происходит при потере сеансового ключа или ключа шифрования данных. Необходим разумный компромисс между вероятностью вскрытия ключа шифрования ключей из-за его слишком длительного использования и возможностью компрометации этого ключа при его передаче абонентам сети. В большинстве случаев разумно ежемесячно, а иногда даже ежегодно, менять ключ шифрования ключей.

Ключи, применяемые для шифрования файлов, которые хранятся на дисках, слишком часто менять не надо. Регулярное повторное шифрование файлов на Новых ключах даст только больше полезной информации криптоаналитику, который будет пытаться их вскрыть. Лучше применить подход, при котором каждый файл шифруется при помощи своего ключа. А сами ключи, в свою очередь, зашифровываются на ключе шифрования ключей, который затем прячут в надежном месте (например, в стальном сейфе).

Что касается открытых ключей, то продолжительность их использования в значительной степени варьируется в зависимости от области применения. Если открытый ключ применяется для целей аутентификации или для цифровой подписи, он продолжает оставаться актуальным годами, иногда даже десятилетиями. Но даже в этом случае не следует пренебрегать сменой ключа каждые 2-3 года, чтобы в распоряжении криптоаналитика накапливалось меньше шифротекста, необходимого для организации атаки. А старый ключ все равно надо продолжать хранить в секрете — он может понадобиться, чтобы, например, подтвердить подлинность подписи, поставленной в течение периода, пока этот ключ был действующим.

Криптографические ключи ни в коем случае не должны попадать в руки противника. Поэтому, как только в ключах отпала надобность, их следует уничтожить. Если ключи хранятся на бумажном носителе, его надо сжечь или пропустить через специальный аппарат для уничтожения бумаг, который должен быть достаточно высокого качества. Ведь будет очень обидно, если ваш алгоритм шифрования, способный выдержать атаку методом грубой силы в течение нескольких миллионов лет, вскроют

только потому, что за несколько десятков тысяч долларов кто-то наймет сотню безработных, и за год они соберут воедино недостаточно тщательно «пережеванный» лист бумаги с записанными на нем ключами.

Если ключ хранился в перепрограммируемом ПЗУ, то необходимо несколько раз записать информацию поверх него. В случае, когда для хранения ключа использовалось ПЗУ, его надо разбить молотком на мелкие кусочки и **равеять** их по ветру. Если ключ лежал на компьютерном диске, на место ключа придется многократно записать ничего не значащие данные или уничтожить диск. При работе на компьютере в многозадачном режиме следует обратить особое внимание на способность операционной системы создавать временные файлы на диске для хранения рабочей копии программы шифрования и ее данных. А сверхосторожный пользователь обязательно напишет программу, которая будет отыскивать копии ключа на свободных секторах диска и удалять их.

Протоколы распределения ключей

Отправитель и получатель сообщений при их взаимодействии в компьютерной сети подчиняются определенным правилам по соблюдению последовательности действий между ними. Такие правила, называемые протоколом, гарантируют не только безопасность сообщений, но и аутентификацию корреспондентов. Поэтому выбор протоколов распределения ключей в сети представляет собой важную проблему.

В настоящее время распределение ключей между пользователями реализуется двумя способами:

- прямым обменом сеансовыми ключами;
- созданием одного или нескольких центров распределения ключей.

В связи с этим возможны следующие ситуации организации обмена ключами:

- прямой обмен ключами;
- обмен через посредника;
- обмен через нескольких посредников.

Как правило, процедура распределения ключей применяется совместно с процедурой проверки подлинности участниковобмена информацией. При этом возможны варианты протоколов распределения ключей с секретным и открытым ключом, то есть на основе **одноключевых** и **двухключевых** методов.

Протоколы распределения ключей с использованием одноключевых методов (с секретным ключом) существуют для двух ситуаций:

- прямого обмена;
- обмена через посредника.

При использовании протокола взаимного обмена с секретным ключом каждое передаваемое сообщение начинается с установления подлинности отправителя. Данный протокол предполагает, что отправитель А и получатель В для подтверждения подлинности сообщения используют секретный ключ **KAB**. Осуществление протокола взаимного обмена сеансовыми ключами К между абонентами происходит в последовательности, отображенной на рис. 4.29.

Получатель сообщения — корреспондент В — посылает запрос **q1** отправителю А на получение сообщения. При этом запрос ql совершенно открыт и может быть послан любым абонентом сети.

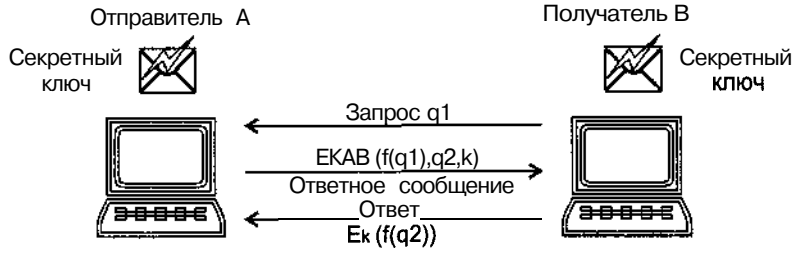


Рис. 4.29. Схема взаимного обмена с секретным ключом

Отправитель сообщения — корреспондент А, получив запрос q1, формирует ответное сообщение, зашифрованное секретным ключом К, где:

- f(q1) — шифрованный запрос q1;
- G q2 — сообщение отправителя А для получателя В;
- К — сеансовый ключ отправителя А.

Получатель В, приняв сообщение, формирует ответ f(q2) и шифрует его с помощью сеансового ключа К отправителя А в виде Ек(f(q2)), что убеждает корреспондента А в достоверности корреспондента В, т. к. им получено сообщение q2 и только они вдвоем знают ключ К.

При использовании протокола обмена ключами через посредника существует некоторое третье лицо (посредник С), которое выполняет только функцию подтвержде-

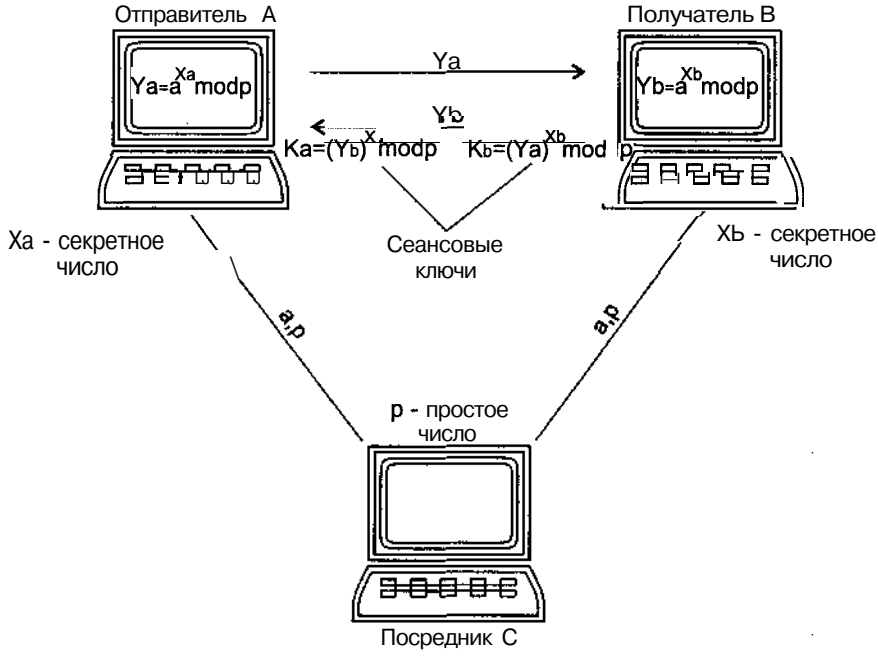


Рис. **4.30.** Протокол передачи ключа по незащищенному каналу

ния подлинности и не должно иметь информации о сеансовых ключах, которыми обмениваются корреспонденты А и В. Такая ситуация соответствует обмену ключами по незащищенному каналу связи (рис. 4.30).

Существующий протокол передачи ключа по неэащищенному каналу используется, как правило, для разделения процедур подтверждения подлинности и распределения ключей. С этой целью посредник С выбирает несекретные числа а и р, снабжает ими корреспондентов А и В (число р — простое число).

Функционирование протокола происходит в следующей последовательности. Пользователь А выбирает секретное число ХА и вычисляет уА. Пользователь В выбирает секретное число ХВ и вычисляет уВ. После этого пользователи А и В обмениваются вычисленными числами уА и уВ. Далее пользователи А и В самостоятельно вычисляют ключи КА и КВ, которые в дальнейшем используются ими в качестве сеансового ключа, и в силу того, выполняется условие — КА = КВ.

Электронная почта

Раньше электронный обмен информацией в стране ограничивался государственными и исследовательскими организациями. В этой среде защита электронного обмена сообщениями не представляла серьезной проблемы. Сегодня в компьютерных сетях электронная почта и другие виды электронного обмена являются важными компонентами современного бизнеса. В связи с этим возрастают требования к обеспечению информационной безопасности финансовых и коммерческих сделок, личной тайны, конфиденциальных данных, передаваемых по сети.

Сейчас вряд ли кто задумывается о том, как же работает электронная почта. Электронная почта (Electronic mail, E-mail) — до сих пор остается одним из самых распространенных и дешевых средств обмена информацией во всех странах мира. Считается, что в мире имеется более 50 млн пользователей электронной почты. Сейчас представить себе работу или просто общение без электронной почты иногда просто невозможно. Она упрощает общение, деловое партнерство или рассылку интересующей информации. И хотя уже существует много других таких Internet-сервисов, как голосовая почта, Internet-телефония или им подобные, но тем не менее стандартная старая добрая и хорошо всем знакомая электронная почта живет. Это вполне естественно, поскольку речь здесь идет просто о передаче порции информации, в подавляющем большинстве случаев текстовой. Это дешевле, чем звонить в другую страну по телефону или использовать голосовую почту, когда объем передаваемой информации на несколько порядков ниже. На самом деле доказывать, что почта хороша и удобна, нет смысла, поскольку всем это понятно и так.

Электронная почта является одним из самых первых сервисов, которые были созданы в Internet. Как и другие сервисы, электронная почта использует в качестве базы протокол IP для передачи информации. Сам же протокол передачи почты называется SMTP и почтовые программы работают уже непосредственно с ним. Это протокол более высокого уровня и, следовательно, более сложный. Важным различием является то, что почта работает непосредственно с пользователями в системе, что накладывает дополнительные требования к защите почтовых систем.

Принцип работы электронной почты очень похож на работу обычной почты. С ее помощью можно посылать сообщения, получать их в свой электронный почтовый ящик, отвечать на письма корреспондентов автоматически, используя их адреса, рассылать копии письма сразу нескольким абонентам, переправлять полученное письмо по другому адресу, создавать несколько подразделов почтового ящика, включать в письма текстовые, аудио- и графические файлы.

Для того чтобы этот обмен информацией между двумя, по крайней мере, абонентами состоялся, необходимо написать послание и, указав адрес, опустить в почтовый ящик, откуда письмо неминуемо попадет на почтовый узел. Если указанный адрес соответствует общепринятым стандартам, то через некоторое время почтальон положит его в почтовый ящик адресата. Далее абонент вскроет послание, и — обмен информацией состоялся. Чтобы ускорить этот процесс, мы поднимаем телефонную трубку, набираем телефонный номер и, если произойдет правильное соединение, то наш абонент услышит то, что мы хотим ему передать. Если абонент не отвечает или его номер занят, придется повторить процедуру еще раз (возможно и несколько раз), сожалея о том, что на это тратится драгоценное время. Исследования показали, что, несмотря на почти мгновенный доступ к телефонной связи, около 75% телефонных вызовов заканчиваются безуспешно. Очень часто нужного абонента просто нет на месте.

Основная привлекательность электронной почты — это быстрота ее работы. Она имеет ту же скорость доступа, что и телефон, но не требует одновременного присутствия обоих абонентов на разных концах телефонной линии, она оставляет письменную копию послания, которое может быть сохранено или передано дальше. Более того, письмо одновременно может быть послано нескольким абонентам. Используя услуги современной электронной почты, можно передавать не только письменные сообщения, а информацию любого рода: фотографии, видео, программы и т. д. И все это гарантированно пересылается в любую точку земного шара за несколько минут.

Принцип функционирования электронной почты

Система современной электронной почты состоит из трех основных компонентов:

- пользовательского агента (User Agent);
- транспортного агента (Transfer Agent);
- доставочного агента (Delivery Agent).

Программы, которые предоставляют пользователям возможность читать и составлять почтовые сообщения, называются пользовательскими агентами. Примеры таких программ — Internet Mail в Windows 95, Netscape, Pine, команда mail в UNIX и многие другие.

Самым первым пользовательским агентом была программа /bin/mail, разработанная в лаборатории AT&T. Сейчас применяются несколько программ этого класса. Кроме того, существуют пользовательские агенты с графическим интерфейсом пользователя. Существует также стандарт, определяющий включение в почтовые сообщения объектов мультимедиа. Он называется MIME (Multipurpose Internet Mail Extensions) — многоцелевые расширения электронной почты для Internet. Данный стандарт поддерживают многие пользовательские агенты.

Пользовательский агент формирует письмо: позволяет написать его текст, присоединить файлы, указать тему письма и все адреса.

Затем письмо передается транспортному агенту — наиболее сложной и важной части почтовой системы. Это программы, которые принимают почту от пользовательского агента, интерпретируют адреса пользователей и переправляют почту на соответствующие компьютеры для последующей доставки. Кроме этого, транспортный агент принимает входящую почту от других транспортных агентов. Транспортный агент отрабатывает протокол SMTP (Simple Mail Transport Protocol) — простой протокол транспортировки почты.

Дойдя до машины второго пользователя, письмо при помощи транспортного агента этой машины передается доставочному агенту (Delivery Agent), который принимает почту от транспортного агента, доставляет ее соответствующим пользователям и отвечает за формирование MailBox пользователя. Обычно MailBox — это файл, где последовательно хранятся все приходящие письма. Почта может доставляться конкретному лицу, в список рассылки, в файл, в программу и т. п. Для обслуживания получателей каждого типа необходим отдельный агент mail — доставочный агент локальных пользователей. На этом работа почтовой системы заканчивается. Из MailBox почта читается почтовыми клиентами (например Netscape), но к работе самой системы это уже отношения не имеет.

Для пересылки любой, в том числе и обычной почты, необходимо знать адрес (нельзя писать письмо «На деревню. Дедушке.»). Это относится и к электронной почте. В системе электронной почты адресация бывает двух видов:

- маршрутно-зависимая;
- маршрутно-независимая.

При использовании первого способа адресации отправитель должен указать промежуточные машины (пункты), через которые должно пройти сообщение, чтобы попасть в пункт назначения и быть доставленным адресату. В адресе второго вида просто указывается пункт назначения. При этом UUCP-адреса являются маршрутно-зависимыми, а Internet-адреса от маршрута не зависят.

UUCP-адрес состоит из списка машин (радиоэлектронного оборудования), через которые должно пройти сообщение на пути к пункту назначения. Элементы списка разделяют восклицательными знаками. Например, в электронно-почтовом UUCP-адресе: mcvax!uunet!ucbvax!hao!boulder!lair!evi — пунктом назначения является машина lair, а получатель — абонент evi. Каждая машина в цепочке имеет непосредственное UUCP-соединение с машинами, которые находятся в сети до и после нее. Например, машина ucbvax должна иметь соединения с машинами hao и uunet. Цепочки UUCP-адресов бывают очень длинными, но теперь, когда широко используется Internet, настоящие громадины увидишь очень редко. Когда электронная почта строилась в основном на базе UUCP, администраторы вынуждены были помнить список компьютеров на довольно больших участках базовой сети UUCP. В формате электронной Internet-почты адрес, приведенный выше, будет иметь вид evi@lair.

Электронно-почтовый Internet-адрес имеет следующий формат:

пользователь@машина,

где знак @ отделяет имя пользователя от обозначения машины.

Рассмотрим в качестве примера адрес электронной почты. Этот адрес (рис. 4.31) содержит идентификатор абонента и сведения о его местоположении. В нашем случае

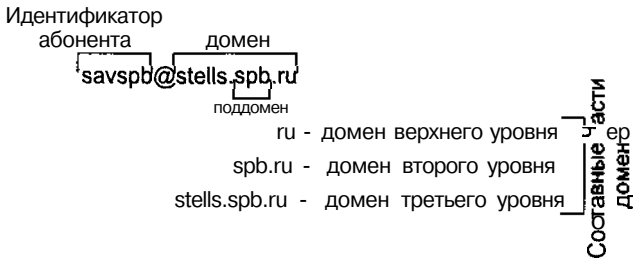


Рис. 4.31. Формат почтового Internet-адреса

идентификатор абонента — savspb. В качестве идентификатора используются имена, фамилии, псевдонимы, очень часто они составляются из начальных букв фамилии, имени, отчества абонента.

То, что стоит справа от знака @, называется доменом и однозначно описывает местонахождение абонента. Домен состоит из составных частей, которые разделяются точками. Самая правая часть домена — это домен верхнего уровня, который, как правило, обозначает код страны адресата. Код страны утвержден международным стандартом ISO. В нашем случае используется код Российской Федерации — ru. Однако в качестве домена верхнего уровня может фигурировать и обозначение сети. Например, в США, где существуют сети, объединяющие высшие учебные заведения или правительственные организации, в качестве доменов верхнего уровня используются сокращения edu — Educational institutions (например, cs.berkeley.edu), gov — Government institutions и др.

Следующая составная часть домена — поддомен является однозначно Определяемым внутри домена верхнего уровня. Нетрудно догадаться (по аналогии с обычным письмом), что после кода страны должен следовать код города — spb в нашем случае однозначно определяет код Санкт-Петербурга. Совокупность составных частей домена spb.ru называется доменом второго уровня. Аббревиатуры домена второго уровня определяются в соответствии с правилами, принятыми доменом верхнего уровня.

Домен третьего уровня — stels.spb.ru. В нашем случае домен третьего уровня включает в себя название фирмы Stels. Правила образования имен внутри доменов третьего уровня — это личное дело доменов второго уровня.

Кроме идентификаторов абонентов, в системе электронной почты используются почтовые псевдонимы, которые позволяют системному администратору и отдельным пользователям переадресовывать почту. Ими можно пользоваться для задания списков рассылки (которые включают нескольких получателей), для пересылки почты между компьютерами и для того, чтобы к пользователям можно было обращаться по нескольким именам. Помимо списков пользователей, псевдонимы могут обозначать:

- ❑ файл, содержащий список адресов;
- ❑ файл, в который должны добавляться сообщения;
- G команду, на вход которой должны передаваться сообщения.

Псевдонимы могут быть определены:

- ❑ в файле конфигурации пользовательского агента;
- О в общесистемном файле псевдонимов /etc/aliases;

- в пользовательском файле пересылки ~/.forward.

Сначала система электронной почты ищет псевдонимы в файле конфигурации пользовательского агента, затем в файле aliases и наконец в пользовательском файле пересылки.

Вот несколько примеров переадресации почты с помощью псевдонимов, определенных в файле aliases:

stels: savspb;
savspb: stels@mailhub;
autors: savspb,som,avit,trent.

В первой строке указано, что почту, поступающую на имя stels, следует доставлять пользователю savspb на локальный компьютер. Во второй, что всю почту, поступающую на имя savspb, следует доставлять на компьютер mailhub. И, наконец, третья строка определяет, что почту, адресованную authors, следует доставлять пользователям savspb, som, avit и trent. Поддерживается рекурсия, поэтому почта, посланная на имя stels, в конце концов, попадает по адресу savspb@mailhub.

Чтобы электронное письмо дошло до адресата, необходимо его оформить в соответствии с международными стандартами и написать стандартизованный почтовый электронный адрес. Общепринятый формат послания определяется документом под названием «Standard for the Format ofARPA — Internet Text messages», сокращенно — Request for Comment или RFC822. Этот формат определяет, что электронное послание должно состоять из текста самого письма и заголовка, который приписывается в начале сообщения. Заголовок отделяется от текста пустой строкой и содержит несколько строчек необходимой информации об этом сообщении: дату отправления, адрес, обратный адрес, тему сообщения и т. д. Каждая из строк заголовка имеет вид: название: текст. Бывает несколько видов строк заголовка. Не все они обязательно должны присутствовать. Некоторые строки почтовые службы добавляют автоматически. (Received: Date:), другие задает сам автор письма (To:, Subject:).

Само письмо состоит из двух частей: заголовка и тела письма. Для системы основным является заголовок, для пользователей — тело письма. Заголовок содержит сведения об авторе письма, о получателях, времени создания. Заголовок также пополняется по мере прохождения письма через сеть, в него заносится информация о том, в какое время письмо проходило и через какие компьютеры. За заголовком следует пустая линия, отделяющая тело письма. В теле прописываются такие важные параметры, как кодировка текста письма, тип присоединенных файлов и некоторые другие. В отличие от многих иных сервисов, письма передаются по сети целиком, но не в том смысле, что одним большим IP-пакетом, а в том, что все пакеты, содержащие письмо, собираются на каждом передающем компьютере. Система передачи полностью аналогична обычному роутингу сетевых пакетов. Для нее применяются записи так называемого Mail eXchanger (MX), которые содержат информацию о том, куда в зависимости от адреса получателя требуется направлять письмо. Так в целом происходит работа почтовых систем.

Рассмотрим пример почтового сообщения:

Received: by avg386.kiae.su; Thu, 20 Dec 90 13:51:59 MSK

Received: by jumbo.kiae.su; Thu, 20 Dec 90 12:52:17 MSK
Received: from CS.ORST.EDU by fuug.fi with SMTP id AA15539 (5.65+/IDA-1.3.5 for avg@kiae.su); Thu, 20 Dec 90 08:19:05 +0200
Received: from jacobs.CS.ORST.EDU by CS.ORST.EDU (5.59/1.15) id AA19981; Wed, 19 Dec 90 22:19:59 PST
Received: by jacobs.CS.ORST.EDU (5.54/1.14) id AA02240; Wed, 19 Dec 90 23:19:35 MST
Date: Wed, 19 Dec 90 23:19:35 MST
From: Harry Brooks <brooksh@jacobs.cs.orst.edu>
Message-Id: <9012200619.AA02240@jacobs.CS.ORST.EDU>
To: avg@kiae.su
Subject: Re: Новое ПО
Status: RO

Привет! Вышли мне описание твоей новой программы.

Received: — это отметка о прохождении через некоторое электронное устройство (своеобразный почтовый штемпель). Количество таких отметок (строчек) показывает, через сколько машин прошло сообщение, чтобы достигнуть адресата. При этом каждая из машин обозначает, когда сообщение проходило через нее (ставит штемпель).

Date: — дата и время отправления письма; они указываются в стандартном формате, поскольку большинство почтовых систем умеют сортировать сообщения по времени.

From: — имя отправителя и обратный адрес, который выделен угловыми скобками.

Message-Id: — внутренний уникальный, единственный в мире идентификатор сообщения, который присваивается почтовой службой отправителя каждому письму. Его можно использовать как исходящий номер для ссылок на письмо.

To: — адрес получателя.

Subject: — тема сообщения. Пометка Re: в этой строке обозначает, что сообщение является ответом (от слова reply) на другое сообщение. У исходного сообщения и у ответа строка Subject: одна и та же. Для ответа почтовая служба автоматически берет тему из исходного сообщения. Это удобно, когда идет длинный разговор на одну тему. Вы сможете потребовать, чтобы почтовая служба отсортировала сообщения по темам, и освежить в памяти предыдущие фразы этого разговора. В этой строке, составляя сообщение, желательно указывать короткое название, но как можно более информативное. Сообщение под заголовком вроде «А помнишь, как-то раз ты мне говорила...» не всякий станет читать.

Status: — статус сообщения; почтовая служба помечает для себя прочитанное сообщение, чтобы второй раз не предложить его как новое.

Само послание — как правило, текстовый файл произвольной формы. При передаче нетекстовых данных (исполняемой программы, графической информации) сообщение перекодируется соответствующими программными средствами. Ввести текст сообщения, сформировать заголовок можно одним из редакторов сообщений для электронной почты.

Характеристика почтовых программ

Для работы с электронной почтой широко используются программы:

- Eudora;
- Microsoft Exchange;
- Internet Mail;
- Outlook Express;
- NETCOMplete;
- Netscape Messenger;
- Pegasus Mail;
- SendMail;
- PostFix;
- Qmail.

Eudora — одна из наиболее распространенных и зависимых от Internet программ. Она может работать с подключением через сеть или удаленный доступ по протоколам PPP и SLIP, а также как программа чтения почты в автономном режиме, полученной для учетной записи интерактивного доступа к оболочке Unix. Большинство наиболее полезных команд Eudora доступны через меню Message.

Программа MS Exchange стала распространяться совместно с операционной системой Windows 95.

С выпуском Office 97 фирмой Microsoft началось распространение новой, улучшенной программы электронной почты — Outlook. Упрощенная и очень удобная в использовании версия Outlook, названная Outlook Express, входит в комплект поставки новой версии браузера Internet Explorer 4.0 компании Microsoft. В отличие от программы Outlook Express, которая предназначена только для обработки сообщений электронной почты и групп новостей, Outlook — комплексная программа, позволяющая проводить обсуждения, составлять расписания, сотрудничать с другими пользователями и т. д.

Internet Mail (она часто распространяется вместе с родственной ей программой Microsoft Internet News или входит в пакет Internet Explorer 3.0) была первой программой Microsoft, действительно нацеленной на Internet. При установке Internet Explorer 4.0 она заменяется программой Outlook Express.

Outlook Express может работать с почтой, передаваемой Internet, локальной сетью и MSN. Запустить эту программу можно двойным щелчком на соответствующей пиктограмме Рабочего стола.

Программный пакет NETCOMplete (бывшая NetCruiser) был разработан компанией фирмой Netcom как для Windows, так и для Macintosh. Он имеет собственную почтовую программу, однако позволяет пользователю работать также и в «посторонних» программах, таких как Eudora, Internet Mail или Pegasus.

Компания Netscape разработала полнофункциональную почтовую программу Netscape Messenger, которая является переработанной версией Netscape Mail.

Pegasus Mail — это широко распространенная почтовая программа, работающая в сетях и через соединения удаленного доступа к Internet.

SendMail — самая первая программа, которая появилась для работы с почтой во всех разновидностях UNIX и соответственно в Linux. Сама программа поставляется бесплатно в виде исходного кода, поэтому перед установкой ее необходимо скомпилировать. Програм-

ма довольно старая, она уязвима с точки зрения защиты, как минимум, по двум причинам. Во-первых, программа не имеет модульной структуры и потому ее исходный код весьма громоздкий. Поскольку она одномодульная, то ничего нового к приведенной выше схеме не добавляется. Во-вторых, хотя программа старая и не всегда надежная, ею пользуются примерно 79% систем. То есть, если какая-то дыра обнаруживается, это делает уязвимым огромное число компьютеров. По мнению многих администраторов сетей, SendMail отживает свое и на смену ей приходят другие, изначально лучше продуманные программы.

Программа PostFix разрабатывалась как альтернатива программе SendMail. Эта программа распространяется бесплатно, поэтому ею пользуются многие. Она совместима с SendMail: поддерживает директории и файлы, стандартные для SendMail. Программа PostFix имеет модульную структуру, каждый модуль запускается независимо от главного, что позволяет не исполнять все части от имени root. Более того, для выполнения какой-то незначительной операции не нужно запускать весь процесс, достаточно запустить ту часть, которая за это отвечает. За счет использования модулей уменьшаются затраты памяти и сокращается время работы. Для обработки писем существуют четыре очереди: maildrop, incoming, active и deferred.

В очередь maildrop попадают письма, уходящие с этого компьютера. Оттуда они передаются в очередь incoming. В нее же попадают все письма с внешних компьютеров. Основная обработка происходит в очередях active и deferred. Active представляет собой письма, обрабатываемые в данный момент. В случае проблем письма не удаляются, а передаются в очередь deferred. Обработка подразумевает определение дальнейшего пути следования письма. Важным свойством этой системы является контроль за соединением с соседними машинами, чтобы гарантировать отсутствие перегрузок системы, скажем, из-за слишком большого числа соединений. Еще один вопрос, который проработан в PostFix гораздо лучше, чем в SendMail, — это защита. Лучшая защита обеспечивается за счет модульности, исполнения критических кусков кода в среде, отделенной командой chroot, и многих других приемов, которые либо просто не применяются, либо по структуре принципиально не подходят программе SendMail.

Конфигурация системы хотя и является сложной, но все же весьма упрощена благодаря программе postconf, позволяющей более-менее наглядно устанавливать новые значения параметров. Существует возможность изменять не все настройки подряд, а только какую-то группу, например параметры, относящиеся к пересылке писем. Основным является файл main.cf. Конечно, его можно редактировать и вручную, но в этом нет особого смысла.

Система QMail является альтернативой программе SendMail и конкурентом программе PostFix. Основные проблемы, которые эта система позволяет решать (в отличие от SendMail), — те же, что и PostFix, то есть модульность, безопасность, удобство настройки. В какой-то мере QMail и PostFix похожи. QMail также бесплатно поставляется в виде исходного кода. Программа QMail предлагает новый формат почтовых ящиков, называемый MailDir. Данный формат позволяет решать некоторые проблемы, которые возникали при работе со старым форматом mbox в критических ситуациях, таких как сбой программы, сбой системного времени или некорректная работа почтовых клиентов, читающих почту.

Как видим, существует много программ для работы с электронной почтой и великое множество путей прохождения электронных сообщений от отправителя до получателя. Особый интерес представляет сервисное обслуживание электронной почты.

Сервисное обслуживание электронной почты

Такой сервис электронной почты, как немедленный обмен сообщениями IM (Instant Messaging), достаточно популярен в современных сетях. Однако реализация приложений на базе IM требует защиты трафика сообщений в случае выполнения следующих задач:

- идентификация;
- разделение файлов;
- отказ в обслуживании.

Если удаленные корпоративные пользователи могут быть надежно идентифицированы, то этого нельзя гарантировать в отношении удаленных (и потенциально неизвестных) пользователей систем обмена сообщениями. Уже было несколько случаев хакерских атак на популярные системы обмена сообщениями, когда они персонифицировали собой сотни пользователей.

Разделение файлов — эта часто имеющаяся у приложений IM возможность, позволяет удаленным пользователям пересылать произвольные файлы на локальный хост по тому же самому соединению, что и график обмена сообщениями. Такие файлы могут быть исполняемыми и часто используются для распространения червей и троянских коней.

Отказ в обслуживании DoS (Denial of Service) связан с тем, что для поддержки приложений IM администратору часто приходится открывать произвольный диапазон портов на брандмауэре, которые могут быть использованы для проведения атак DoS.

Определенный скептицизм в отношении защиты IM состоит в том, что сеть не заслуживает доверия и что информация может подвергнуться перлюстрации и злонамеренной модификации со стороны злоумышленников. В связи с этим для IM могут быть выделены три опасности:

- подсматривание (stalking);
- подделка (spoofing);
- спам (spamming).

Подсматривание — это перехват данных IM при их передаче по Internet с целью определения местонахождения сети участника обмена в реальном времени. В настоящее время соответствующие организации работают над необходимыми протоколами контроля доступа и обеспечения невидимости.

Подделка — изменение данных сообщения, а также подмена имени (имперсонификация) отправителя. Достоверность сообщения и отправителя можно обеспечить за счет использования надежных идентификационных и криптографических дайджестов сообщений.

Спам — получение сорных сообщений, борьба с которыми — общая проблема для мира асинхронного обмена сообщениями. Задача состоит в создании набора правил доставки для блокирования сорных сообщений.

Рассмотрим еще один новый сервис сети — систему унифицированного обмена сообщениями (Unified Messaging, UM). Наверное, вам приходилось сталкиваться со следующей рекламой услуг (часто бесплатных): «Факсимильные, голосовые, пейджинговые, сотовые и электронные сообщения в одном легко доступном почтовом ящике Internet!». Предпосылка проста: использовать повсеместность Internet для доступа к нескольким разновидностям сообщений с помощью единого метода, часто на базе Web.

Системы унифицированного обмена сообщениями имеют двоякую цель: получение доступа к сообщениям из любой точки и сокращение расходов на связь за счет извлечения сообщений из «универсального почтового ящика» с использованием имеющихся локальных бюджетов доступа в Internet.

Нет сомнения, что мечты об унифицированном почтовом ящике вскоре станут реальностью, однако эта концепция таит зловещие последствия для корпоративной защиты.

В настоящее время стандартов на UM практически нет. Их отсутствие вынуждает производителей предлагать собственные нестандартные решения. В свою очередь это усложняет защиту всех протоколов, особенно для тех унифицированных сервисов, где применяется несколько методов сбора сообщений.

Возьмем, к примеру, ситуацию, когда отдел кадров посылает вам факс с условиями вашего грядущего повышения (включая информацию об окладе и предоставляемых акциях). Если даже отправитель пользуется (относительно) закрытой средой, то сам факс может быть помещен в нешифруемый цифровой почтовый ящик на узле провайдера. Хотя аналоговые голосовые сообщения оцифровываются для их извлечения с помощью электронной почты Internet, это еще не означает, что они шифруются. Например, факс из соседнего отдела может просто храниться в одном из широко распространенных графических форматов (TIFF, JPG и т. п.).

При отсутствии ясных и исчерпывающих протоколов защиты, охватывающих все технологии доступа UM, следует все данные рассматривать как «чрезвычайно конфиденциальные». Если ваша политика защиты предусматривает одинаковый подход ко всем данным UM, то с ними нужно обращаться так, как если бы они были наиболее важными и наименее защищенными. Некоторые сообщения в результате могут оказаться зашифрованными дважды, но это небольшая плата по сравнению с возможными последствиями.

Способы информационной защиты электронной почты

Секретные агенты в голливудских боевиках все больше предпочитают электронную почту обычной. Между тем, рассылка деловых писем или личных сообщений по электронной почте совершенно не добавляет им секретности. Для простоты представьте, что детали сделки или подробности своей интимной жизни вы посылаете на открытке, которую могут прочитать все желающие. По оценкам экспертов, лишь одно из ста писем удовлетворяет требованиям безопасности. При этом не думайте, что вы станете объектом внимания, только если займете высокий пост или заработаете несколько миллионов долларов. Системный администратор вашей компании, например, может беспрепятственно просматривать личную почту на предмет соблюдения секретов фирмы или просто из любопытства. Кроме этого существует еще много Способов, если уж не вскрыть вашу почту, то по крайней мере ее испортить или не дать достигнуть адресата. Рассмотрим, что может угрожать электронной почте.

Наиболее очевидным следствием полномасштабной реализации обмена сообщениями является необходимость управлять его информационным наполнением. Если надежность источника и содержания факсимильного документа и голосовой почты не вызывает сомнения, то борьба за обеспечение целостности сообщений электронной почты продолжается.

Решение задач управления информационным наполнением считается успешным при соблюдении:

- конфиденциальности;
- целостности.

Обеспечить конфиденциальность обмена электронной почтой просто только теоретически; при практической реализации — это весьма трудная задача, в том числе и с точки зрения управления.

Недавние инциденты с вирусами Melissa и Love Bug продемонстрировали реальную угрозу: сегодня в глобальной сети Internet один вирус может поразить миллионы хостов практически по всему миру.

Несмотря на глобальный характер угрозы, защита должна быть организована локально, и бдительный администратор сети должен подготовить продуманный план защиты. Большинство предприятий имеет брандмауэры с поддержкой анализа информационного наполнения (с активными фильтрами для выявления известных вирусов), однако они абсолютно не надежны, как о том свидетельствует недавний всплеск атак с применением троянских коней.

Помимо активного мониторинга, администратор защиты может подготовиться к вирусным атакам на электронную почту, приняв следующие меры:

- обеспечить оперативное информирование пользователей при обнаружении атаки;
- использовать адаптивную фильтрацию подозрительной почты;
- периодически информировать пользователей об изменениях в политике защиты и обращении с вирусами, включая процедуру оповещения об инцидентах;
- внедрить адекватные процедуры резервного копирования и восстановления данных.

Обеспечение оперативного информирования, как только атака будет обнаружена, должно включать широковещательную рассылку предупреждений как традиционными, так и электронными средствами, развешивание объявлений, указание корпоративного URL, где пользователи могут найти информацию, предоставление четких кратких инструкций, как поступать с вирусом, указание координат ответственного сотрудника отдела информационных систем. Однако возможные последствия инцидента не следует преувеличивать, но и не стоит притуплять чувство опасности, так как это может иметь отрицательные последствия в случае чрезвычайной вирусной угрозы.

С помощью адаптивной фильтрации подозрительной почты во время последних инцидентов в большинстве компаний смогли отфильтровывать как входящие, так и исходящие сообщения со словами «I Love You» в теме сообщения (фирменный знак этих вирусов). Кроме того, сообщения рекомендуется ограничивать по размеру, по крайней мере, на первое время после обнаружения опасности. Это поможет воспрепятствовать распространению сомнительных вложений, таких, как исполняемые файлы. Порог в 5 кбайт является достаточным.

Благодаря периодическому информированию пользователей об изменениях в политике защиты и обращении с вирусами, включая процедуру оповещения об инцидентах, можно заранее дать пользователям инструкции, как вести себя в случае атаки. Кроме того, их следует проинструктировать относительно необходимости регулярно-

го обновления файлов с сигнатурами вирусов. Наконец, пользователей было бы неплохо научить отличать реальные вирусы от их имитаций.

Внедрение адекватных процедур резервного копирования и восстановления данных необходимо на случай применения вирусов, которые не используют макросы или исполняемые файлы для проникновения в систему. Такие атаки часто заставляют пользователей удалить все сообщения из почтового ящика или, возможно даже, содержимое всего жесткого диска. Общие сетевые разделы позволяют централизовать резервное копирование, однако эти диски должны быть тщательно разграничены между собой, чтобы вирусы не распространялись дальше.

Защита от вирусов и троянских коней составляет отдельную самостоятельную задачу, однако настоящую опасность представляют менее явные угрозы: кража интеллектуальной собственности, снижение продуктивности и даже ответственность за неправомочное использование корпоративных ресурсов. Система анализа информационного наполнения — один из множества инструментов, который следует реализовывать для соблюдения политики компании в отношении электронной почты.

Все методы извлечения информации должны быть защищенными. Выполните анализ защиты всех методов сбора сообщений и периодически проверяйте каждую среду доступа (включая беспроводную и телефонную связь). К примеру, еще в 1997 году шифровальщик Брюс Шнайер (из Counterpane Lab) обнаружил «дыру» в технологии шифрования, используемой в цифровых сотовых телефонах.

Не следует применять нестандартные или новые технологии, в них может быть множество «дыр». Стандартные протоколы необходимо постоянно испытывать на предмет надежности защиты, в результате чего они становятся эффективнее.

Самый очевидный выход из создавшегося положения — шифрование. Почему же этот способ не получил распространения, и все письма в Internet не кодируются автоматически? В первую очередь, из-за наличия разных стандартов. Два наиболее популярных способа шифрования — S/MIME (Secure Multipurpose Internet Mail Extension) и PGP (Pretty Good Privacy) — несовместимы друг с другом.

Тем не менее, секретное электронное письмо не только шифруют, но и заверяют цифровой подписью. Таким образом, вы совершенно точно будете знать, от кого именно это письмо, что его содержание не было изменено и, более того, не было прочитано. Защита сообщения происходит с помощью двух цифровых комбинаций, называемых личным и открытым ключами. Личный ключ хранится на вашем компьютере, и никто кроме вас доступа к нему не имеет. Открытый ключ общедоступен, например, на вашей домашней странице.

Вы пишете письмо другу и шифруете его своим секретным ключом. Друг расшифровывает его с помощью вашего открытого ключа. Таким образом, он уверен, что письмо прислали именно вы и что его содержание не подменили, так как шифрующий ключ есть только у вас. Но такое сообщение еще можно перехватить и прочитать. Для полной защиты вам необходимо поверх шифровки собственным ключом зашифровать письмо открытым ключом вашего друга. Тогда он будет единственным, кто может прочитать сообщение.

Вероятность расшифровки и подмены подобного письма очень мала. Правда, появляется необходимость регулярно проверять актуальность чужих ключей — не были ли они изменены или скомпрометированы (например, украдены). Для этого служат

компании, подтверждающие актуальность ключа. К тому же вы вправе потребовать от подобной компании цифровой ключ, подтверждаемый другой компанией, и т. д. Подобная иерархия компаний, подтверждающих ключи друг друга, с самой авторитетной компанией наверху реализована в протоколе S/MIME. PGP использует для этих же целей Сеть доверия (Web of Trust), состоящую из общих друзей и знакомых.

Очевидно, что ввиду расширения использования электронного обмена сообщениями в бизнесе этот сервис должен быть также надежным и защищенным. Однако, будучи, наверное, самым распространенным сетевым приложением, электронный обмен сообщениями часто является и самым незащищенным.

Как правило, если только обмен не происходит по частной сети или VPN, единственный способ гарантировать конфиденциальность состоит в шифровании сообщения на рабочей станции отправителя и последующей ее дешифровки на станции получателя.

Для достижения этой цели предлагаются, по крайней мере, три конкурирующих подхода, каждый на базе соответствующих протоколов. Первый подход опирается на Secure/MIME (S/MIME) компании RSA Security. Это расширение протокола кодирования MIME. S/MIME стал форматом де-факто для двоичных мультимедийных вложений в электронные сообщения. Хотя первый протокол S/MIME был разработан RSA, текущая версия S/MIME базируется на спецификации IETF (RFC 2632,2633 и 2634) и, таким образом, представляет собой открытый стандарт.

Благодаря включению сообщений в формате стандарта на криптографию с открытыми ключами PKCS7 (Public Key Cryptography Standart #7) в тело MIMI протокол S/MIME позволяет получателю идентифицировать личность отправителя с помощью шифрования с открытыми ключами. При таком подходе подпись сообщения просто сравнивается с открытым ключом отправителя.

S/MIME — наиболее широко распространенный способ сквозной защиты информационного наполнения. Он пользуется поддержкой основных поставщиков протоколов для обмена сообщениями, включая Microsoft, Lotus, Netscape (Communications и Novell).

Второй подход к обеспечению конфиденциальности электронной почты (Pretty Good Privacy, PGP) был предложен Филиппом Циммерманом в виде бесплатного инструментария для UNIX, однако впоследствии его коммерческой реализацией занялась Network Associates, и теперь PGP доступен и для платформ Windows и Macintosh.

Хотя PGP мог применяться к составным вложениям сам по себе, имеющиеся предложения ориентируются на MIME как на структуру информационного наполнения и поэтому называются PGP/MIME. Кроме того, IETF в настоящее время работает над открытой версией PGP, называемой OpenPGP.

Как и S/MIME, спецификация PGP предполагает шифрование сообщений с использованием симметричного ключа (один и тот же ключ применяют как для шифрования, так и для дешифровки данных), после чего он присоединяется к сообщению и шифруется с помощью технологии с открытыми ключами. Это исключает необходимость шифрования текста сообщения посредством открытого ключа — весьма медленного процесса.

Однако в отличие от S/MIME, технология PGP не предусматривает иерархического распространения (и подписи) открытых ключей. Вместо этого PGP опирается на концепцию «паутины доверия», в соответствии с которой пользователь получает

открытые ключи надежными средствами (например, лично) и затем самостоятельно решает относительно принятия других ключей, подписанных теми же доверенными уполномоченными. Такой механизм прост для реализации на корпоративном уровне, но ему недостает масштабируемости иерархических PKI (Public-key Infrastructure).

Третий подход составляет совокупность PEM (Privacy Enhanced Mail) и MOSS (MIME Object Security Services). Задуманный еще в 1993 году, протокол PEM стал первой попыткой защитить обмен электронной почтой; он был опубликован IETF в качестве проекта стандарта в RFC 1421,1422,1423 и 1424. Однако его существенным недостатком была неспособность обрабатывать восьмибитовые текстовые сообщения (что необходимо для мультимедийных вложений), поэтому спецификация MOSS и была предложена в качестве замены PEM.

На сегодняшний день и PEM, и MOSS остаются, однако, высокоуровневыми спецификациями; мало кто прилагает усилия для достижения совместимости между конкурирующими реализациями. Стандарты на защиту обмена сообщениями продолжают совершенствоваться, а тем временем уже начинают постепенно вырисовываться наилучшие способы защиты.

У компьютерной отрасли есть вполне обоснованная надежда, что реально совместимая модель защиты появится в скором будущем и будет она столь же зрелая, как и сами почтовые транспортные протоколы.

Фантастически быстрый успех многих компаний, предлагающих новые технологии для Internet, связан, как правило, с изобретением нового Web-сервиса, полезность которого для широкой аудитории настолько очевидна, что число его пользователей достигает десятков миллионов человек. Так было, в частности, с бесплатной регистрацией почтовых адресов в Hotmail. Для работы с подобными системами не требуется никакого клиентского программного обеспечения, кроме браузера, абоненты не привязаны жестко к своему провайдеру и могут пользоваться электронной почтой в любом месте, оборудованном Web-терминалом. Несмотря на очевидные достоинства, одна важная проблема не решена и здесь. Речь идет о защищенности передаваемой корреспонденции от посторонних глаз.

Сложность задачи заключается не в алгоритмах шифрования, которые известны и достаточно хорошо проработаны, а в организации удобной работы с ключами, в преодолении строгих юридических рогаток и, самое главное, в завоевании доверия клиента. Хорошо известно, что в США установлены очень жесткие ограничения на экспорт стойких средств шифрования, за смягчение которых борются не только защитники прав и свобод человека, но и ведущие производители прикладных информационных систем, потому что их продукция теряет свою конкурентоспособность на мировом рынке. ФБР и ЦРУ лоббируют принятие законов, регламентирующих предоставление государственным органам по решению суда секретных ключей, выданных клиентам уполномоченными на это организациями. И хотя приводимые аргументы (борьба с терроризмом и контроль над государствами, не признающими решений мирового сообщества) выглядят убедительно, не только преступники, но и законопослушные субъекты хотели бы иметь дополнительные гарантии сохранения конфиденциальности своей корреспонденции.

Поддержка всеми современными браузерами протокола SSL (Secure Socket Layer), обеспечивающего шифрование данных в процессе их передачи из одного узла в дру-

гой, проблемы не решает, т. к. после этого почтовые сообщения хранятся на серверах в незашифрованном виде.

В ZipLip.com пошли по простому пути: переданное с помощью SSL сообщение не дешифруется и хранится на почтовом сервере до тех пор, пока за ним не обратится получатель. Соответствующий ключ генерируется на основе фразы-пароля, которая должна быть заранее известна и отправителю, и получателю. Поскольку шифрование происходит на сервере, находящемся на территории США, экспортные ограничения не нарушаются, и длина ключа может быть любой. С другой стороны, из-за того что ключ хранится вместе с зашифрованным сообщением, получить доступ к нему могут не только представители ФБР, но и сотрудники ZipLip. Таким образом, в этом случае все сводится к проблеме доверия.

В основе решения HushMail лежит более изощренный подход. Поскольку оно базируется на технологии Java (JVM 1.5.5 и более поздние редакции), в качестве почтовых клиентов можно использовать лишь достаточно свежие версии Web-браузеров: Netscape Navigator (начиная с версии 4.04) и Internet Explorer (начиная с версии 4.5). Благодаря применению средств шифрования с открытым ключом корреспонденты не обязаны знать и помнить чужие пароли. На разных этапах используются симметричные и несимметричные алгоритмы шифрования. Напомним, что при симметричном шифровании один и тот же ключ служит как для кодирования, так и для декодирования, а при несимметричном — кодирование осуществляется открытым ключом, а декодирование — секретным,

Специалисты Hush Communications приложили немало усилий, чтобы, с одной стороны, максимально упростить процедуру генерации ключей, а с другой — сделать их недоступными для посторонних лиц (в том числе и государственных органов) без разрешения владельца. При этом многие правовые коллизии были решены столь тонко, что представитель ФБР был вынужден признать легитимность системы HushMail, посетовав на то, что она выводит передаваемую корреспонденцию из под юридического контроля.

При регистрации пользователя в HushMail пара ключей (открытый и секретный) генерируется непосредственно на его клиентской машине. Для этого туда загружается специальный Java-апплет, который предлагает пользователю случайным образом поманипулировать мышью, а затем на основе зафиксированной и рандомизированной последовательности координат формирует пару ключей (длиной 1024 бит). Сообщение шифруется специальным апплетом, пересылаемым с сервера HushMail на браузер клиента. Понимая, что строгие судьи могут квалифицировать загрузку апплета как некую форму незаконного экспорта криптографического программного обеспечения, Hush Communications разместила свой сервер за пределами США (по разным сведениям, в Канаде или на расположенном в Карибском бассейне острове Ангвилла). Кроме того, сами апплеты были разработаны гражданами Ангвиллы — своеобразной программистской оффшорной зоны с весьма мягким законодательством в отношении средств шифрования.

Открытый ключ пересылается на сервер HushMail, откуда он автоматически выдается другому клиенту системы HushMail, написавшему секретное письмо данному пользователю. Таким образом, в конфиденциальной переписке могут принимать участие лишь зарегистрированные пользователи HushMail.

В описанной конфигурации, когда секретный ключ хранится на компьютере пользователя, компания Hush Communications вообще не имеет никакого доступа к секретным ключам своих клиентов и поэтому будет не способна их выдать кому-либо даже при наличии официальной судебной санкции. Однако в этом случае теряется одно из главных преимуществ Web-почтовых систем: возможность получения и пересылки корреспонденции с любого компьютера, подключенного к Internet.

Указанная проблема решается следующим образом. Еще на этапе регистрации апплет предлагает пользователю задать достаточно длинную фразу-пароль, которую тот должен хорошо запомнить. На основе пароля генерируется симметричный 128-разрядный ключ, с помощью которого секретный ключ шифруется и отправляется на хранение на сервер HushMail. Теперь, независимо от местонахождения, вы можете подключиться к HushMail и загрузить с сервера свой дополнительно зашифрованный секретный пароль.

Далее все повторяется в обратном порядке: апплет просит вас ввести фразу-пароль, генерирует на ее основе тот же самый 128-разрядный симметричный ключ, расшифровывает секретный пароль, а уже с его помощью — зашифрованное письмо. Реальная процедура организована немного сложнее: пара ключей (открытый/секретный) используется для кодирования не самого письма, а одноразового симметричного 128-разрядного ключа, с помощью которого шифруется письмо, но это не принципиально.

Итак, все потенциально опасные для пользователя операции — генерация ключей, шифрование и декодирование сообщений — осуществляются на его клиентской машине вдали от сервера HushMail. Сообщения и секретные ключи хранятся на нем в зашифрованном виде и не могут быть вскрыты без фразы-пароля. Тем самым специалисты Hush Communications лишний раз хотят убедить всех в том, что защита корреспонденции обеспечивается не их «клятвами», а объективной изоляцией критически важных ключей.

Протоколы аутентификации в компьютерных сетях

Протоколы аутентификации пользователей

Существует два основных вида протоколов аутентификации в компьютерных сетях:

- аутентификация пользователя;
- аутентификация данных.

Аутентификация пользователя представляет собой процесс подтверждения его подлинности с помощью предъявляемого им аутентификатора.

Аутентификатор, в свою очередь, — это средство аутентификации, характеризующее отличительный признак пользователя. В качестве аутентификатора в компьютерных сетях обычно используются пароль и биометрические данные пользователя (отпечатки пальцев, рисунок сетчатки глаза, тембр).

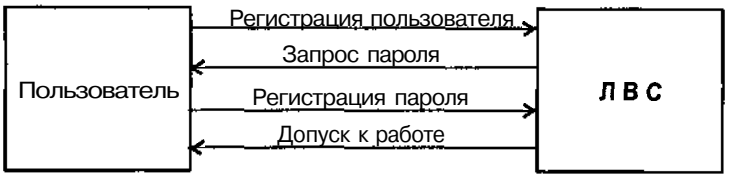


Рис. 4.32. Схема аутентификации пользователя с простым паролем

Пароль представляет собой кодовое слово в буквенной, цифровой или буквенно-цифровой форме, которое вводится в компьютер перед началом диалога.

В современных компьютерных сетях каждый пользователь снабжается паролем и идентификатором с целью подтверждения подлинности пользователя для допуска его к работе в сети. В связи с этим разрабатываются протоколы аутентификации пользователей. Наиболее простые из них формируются с использованием простых паролей или изменяющихся паролей из созданного списка паролей.

Суть протокола аутентификации пользователя с простым паролем заключается в следующем (рис. 4.32). В начале сеанса работы пользователь передает в компьютерную сеть свой идентификатор и регистрируется. После этого сеть запрашивает его пароль. Он отправляет пароль в компьютерную сеть, где и происходит регистрация пароля. Если идентификатор в компьютерной сети зарегистрирован, а пароль верен, то пользователь допускается к работе в сети.

Данный протокол аутентификации пользователя является наиболее простым и слабо защищенным от злоумышленника. Идентификаторы пользователей не представляют большого секрета среди своих сотрудников, а пароль может узнать другой пользователь, имеющий больше прав доступа.

Протокол аутентификации пользователя на основе списка паролей более защищен от злоумышленника, так как применяется список паролей, изменяющихся в соответствии с порядковым номером вхождения в компьютерную сеть. При этом пользователь и сеть обладают списком паролей. Суть работы данного протокола заключается в следующем (рис. 433). При первом вхождении в компьютерную сеть пользователь передает ей свой идентификатор. Сеть запрашивает первый пароль из списка паролей. Последний в соответствии со списком паролей выбирает первый пароль и отправляет его в компьютерную сеть, после чего, если пароль правильный, получает разрешение на допуск к работе. В случае повторного запроса на допуск к работе из списка паролей выбирается второй пароль и т. д.

Среди недостатков данного протокола следует отметить необходимость запоминать длинный список паролей, а также неопределенность выбора пароля при сбоях в линиях связи.

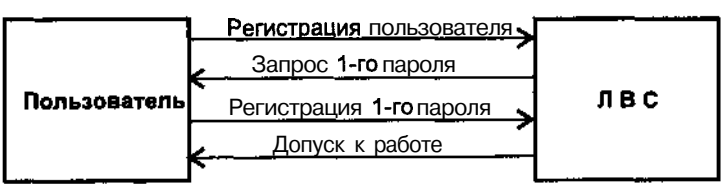


Рис. 4.33. Схема аутентификации пользователя на основе списка паролей

Аутентификация данных — это процесс подтверждения подлинности данных, предъявленных в электронной форме. Данные могут существовать в виде сообщений, файлов, аутентификаторов пользователей и т. д. В настоящее время аутентификация данных в компьютерных сетях основана на использовании электронно-цифровой подписи (ЭЦП). Рассмотрим более подробно принципы использования ЭЦП в компьютерных сетях.

Необходимость использования электронной цифровой подписи

В чем же состоит определение подлинности (аутентификация) информации? Прежде всего в установке того факта, что полученная информация была передана подписавшим ее отправителем, и что она при этом не искажена.

Сегодня нетрудно констатировать, что электронные технологии идут вперед с головокружительной скоростью. Словосочетание «электронная цифровая подпись» стало уже привычным. А еще сравнительно недавно пользователи с большим недоверием относились к электронным документам, считая, что подделать их проще, чем документы на бумажном носителе.

Собственноручная подпись под документом с давних пор используется людьми в качестве доказательства, что человек, подписавший данный документ, ознакомился с ним и согласен с его содержанием. Почему же подпись заслужила такое доверие? Основные причины этого заключаются в следующем:

- подлинность подписи можно проверить (ее присутствие в документе позволяет убедиться, действительно ли он был подписан человеком, который обладает правом ставить эту подпись);
- подпись нельзя подделать (подлинная подпись является доказательством того, что именно тот человек, которому она принадлежит, поставил эту подпись под документом);
- подпись, которая уже стоит под одним документом, не может быть использована еще раз для подписания второго документа (подпись — неотъемлемая часть документа и ее нельзя перенести в другой документ);
- подписанный документ не подлежит никаким изменениям;
- от подписи невозможно отречься (тот, кто поставил подпись, не может впоследствии заявить, что он не подписывал этот документ).

На самом деле, ни одно из перечисленных свойств подписи полностью, на все 100%, не выполняется. В нашем современном криминальном обществе подписи подделывают и копируют, от них отрекаются, а в уже подписанные документы вносят произвольные изменения. Однако люди вынуждены мириться с недостатками, присущими подписи, поскольку мошеннические трюки с подписями проделывать не просто и шансы быть пойманными у мошенников достаточно велики.

Проблему электронной подписи можно было бы решить путем создания сложных считывающих устройств, разлагающих подпись на бумаге на элементы, переводящих эти элементы в цифровой код и на приемном конце производить операцию проверки подлинности, сверяя полученный цифровой код с хранящимся образцом. Такие технические средства уже используются, но, в основном, для защиты от несанкционирован-

ного доступа, где пользователь ставит свою подпись и в его присутствии происходит сверка. Совсем иначе обстоят дела, если документ послан по почте. При этом возникает трудная проблема: подписанный документ можно перехватить и изменить или полностью заменить, и к поддельному документу «приклеить» подпись, «отрезанную» от подлинного.

Попытка использовать подпись в компьютерных файлах сопряжена с еще большими трудностями по тем причинам, что:

- любой файл можно скопировать вместе с имеющейся в нем подписью;
- после подписания в файл можно внести любые изменения, которые в принципе не поддаются обнаружению.

Эти недостатки устраняются при использовании электронной цифровой подписи, позволяющей заменить при безбумажном электронном документообороте традиционные печать и подпись. Она не имеет ничего общего с последовательностью символов, соответствующих печати или подписи, приписанной к документу. При построении цифровой подписи вместо обычной связи между печатью или рукописной подписью и листом бумаги выступает сложная зависимость между документом, секретным и общедоступным (открытым) ключами, а также цифровой подписью. Невозможность подделки электронной цифровой подписи обусловлена очень большим объемом математических вычислений.

Эта подпись может иметь вполне читаемый, «буквенный» вид, но чаще она представлена в виде последовательности произвольных символов. Цифровая подпись может храниться вместе с документом, например, стоять в его начале или конце, либо в отдельном файле. Естественно, что в последнем случае при проверке подписи необходимо располагать как самим документом, так и файлом, содержащим подпись.

Чего мы хотим от электронной цифровой подписи и чем она лучше обычной? Электронная цифровая подпись — это средство, позволяющее на основе использования криптографических методов определить авторство и подлинность документа. При этом электронная цифровая подпись имеет следующие преимущества:

- возможность идентификации принадлежности подписи на основе объективных показателей;
- высокая защищенность от подделки;
- жесткая связь с подписываемым документом.

Если первые два условия еще можно как-то реализовать для традиционной подписи, то третье выполняется только в случае применения электронной цифровой подписи. Ведь она представляет собой специальный зашифрованный код, присоединяемый к электронному сообщению. Это еще и один из самых перспективных способов аутентификации и установления доверительных связей на рынке электронной коммерции. Но до сих пор не существует единого мнения о том, какой способ шифрования наилучший и как организовать сети, где используются цифровые подписи. Но и в случае применения цифровой подписи существуют «подводные камни», угрожающие электронным документам.

Рассмотрим возможные угрозы (виды злоумышленных действий), которые наносят существенный ущерб развитию электронного документооборота. Они подрывают доверие к компьютерной технологии визирования документов. При обмене электронными документами (рис. 4.34) существуют следующие виды злоумышленных действий:

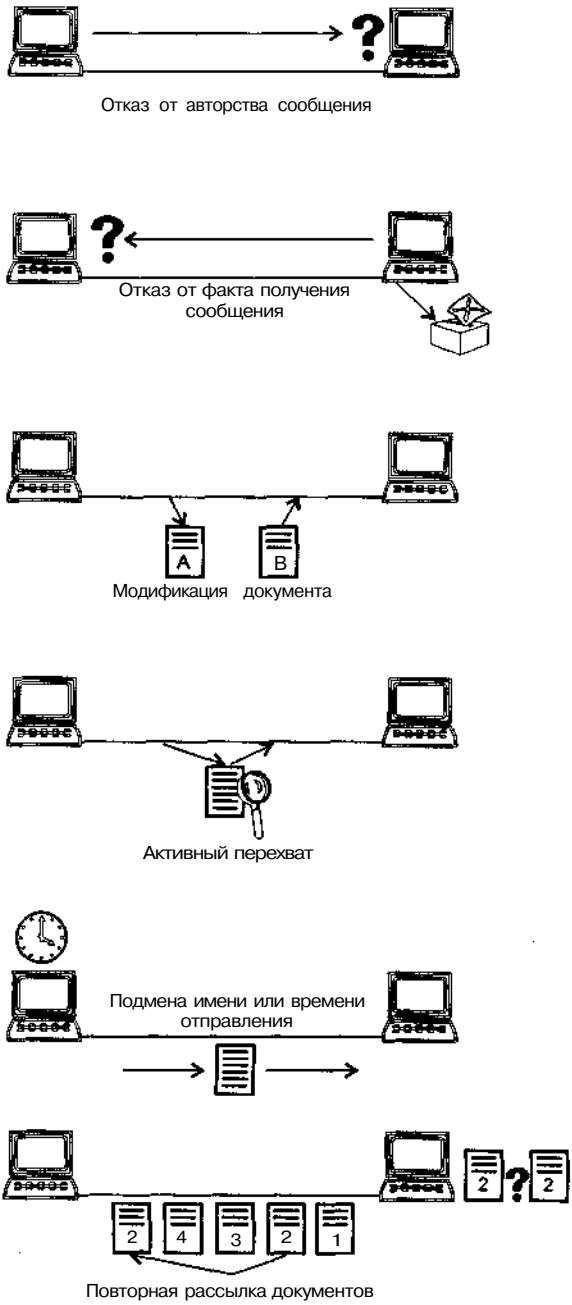


Рис. 4.34. Виды злоумышленных действий с электронными документами

- отказ от авторства или от факта получения документа;
- модификация документа;
- подмена документа;
- активный перехват;
- подмена имени («маскарад»);
- повторная рассылка документов.

В случае отказа от авторства пользователь А заявляет, что не посылал документ пользователю В, хотя на самом деле послал. При модификации документа пользователь А сам изменяет полученный документ и утверждает, что именно таким получил его от пользователя В. Когда пользователь В формирует документ и заявляет, что получил его от пользователя А, имеет место подмена документа. Если злоумышленник подключился к сети, он активно перехватывает информацию и вносит в нее изменения. В ситуации, когда пользователь С посылает документ не от своего имени, а от имени пользователя А, имеет место подмена имени или так называемый «маскарад». При повторной рассылке документов пользователь С повторяет посылку документа, который пользователь А ранее послал пользователю В. Для этого, чтобы исключить возможность подобных злоумышленных действий, и придумали электронную цифровую подпись.

При выборе алгоритма и технологии аутентификации необходимо предусмотреть надежную защиту от всех перечисленных видов злоумышленных действий. Однако в рамках классической (одноключевой) криптографии защититься от угроз всех этих видов трудно, по-

скольку имеется принципиальная возможность злоумышленных действий одной из сторон, владеющих секретным ключом.

Никто не может помешать пользователю, например, создать любой документ, зашифровать его с помощью имеющегося ключа, общего для двух пользователей, а потом заявить, что он получил этот документ от него.

Значительно эффективнее работают схемы, основанные на использовании двухключевой криптографии. В этом случае каждый передающий пользователь имеет свой секретный ключ, а у всех других пользователей есть несекретные открытые ключи передающих абонентов. Эти открытые ключи можно трактовать как набор проверочных соотношений, позволяющих судить об истинности подписи передающего пользователя, но не позволяющих восстановить секретный ключ подписи. Передающий пользователь несет единоличную ответственность за свой секретный ключ. Никто, кроме него, не в состоянии сформировать корректную подпись. Секретный ключ передающего пользователя можно рассматривать как его личную печать, и ее владелец должен всячески ограничивать доступ к ней.

Таким образом, электронная цифровая подпись представляет собой некое достаточно длинное число, полученное в результате преобразования электронного образа защищаемого документа с использованием секретного (личного) ключа отправителя. Любой может проверить стоящую под документом электронную цифровую подпись при помощи соответствующих преобразований с использованием опять-таки электронного образа документа, открытого (публичного) ключа отправителя и собственно значения ЭЦП. Открытый и секретный ключи однозначно связаны между собой, однако невозможно вычислить секретный ключ по открытому. Точнее, если формулировать совсем строго, то пока не найдено алгоритмов, позволяющих сделать такие вычисления за приемлемое время с учетом современного уровня развития техники и используемой длины ключей.

Криптостойкость цифровой подписи должна обеспечивать трудность ее подделки любым человеком, не имеющим доступа к секретному ключу. Причем трудоемкость подделки должна быть велика как для совершенно постороннего пользователя, так и для участника данной сети и не зависеть от числа подписанных документов, перехваченных злоумышленником. Кроме того, на нее не должно влиять то, что у злоумышленника есть возможность готовить документы «на подпись» отправителю. Причем должна обеспечиваться соответствующая защита от несанкционированного доступа к хранящемуся секретному «образцу подписи».

Реализация цифровой подписи

Чтобы поставить цифровую подпись под конкретным документом, необходимо проделать довольно большой объем вычислений. Эти действия осуществляются в два этапа:

О генерация ключей;

❑ подписание документа.

При использовании несимметричного шифрования, а именно его и применяют для цифровой подписи, каждый абонент, обладающий правом подписи, самостоятельно на своем компьютере формирует два ключа подписи: секретный (собственный) и открытый (общий).

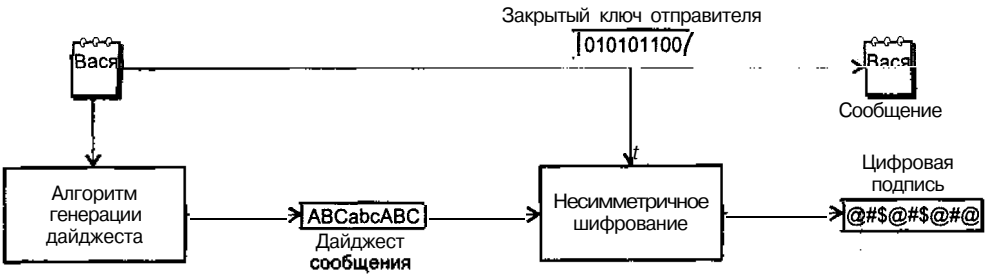


Рис. 4.35. Реализация ЭЦП

Секретный ключ применяют для выработки подписи (рис. 4.35). Только секретный ключ гарантирует невозможность подделки злоумышленником документа и цифровой подписи от имени заверяющего. Никто, кроме владельца, не сможет сформировать ЭЦП под документом. Зато любой может проверить (с помощью доступного всем открытого ключа), что документ подписал именно владелец и что документ не искажен (так как значение ЭЦП зависит и от содержимого документа). Логичное следствие состоит в том, что невозможно просто перенести ЭЦП с одного документа на другой (по аналогии с ксерокопированием или сканированием обычной подписи на бумажном документе или использованием факсимиле). Таким образом, можно сказать, что электронная цифровая подпись является реквизитом данного конкретного электронного документа.

Открытый ключ вычисляется как значение некоторой функции от секретного, но знание открытого ключа не дает возможности определить секретный ключ. Открытый ключ можно опубликовать и использовать для проверки подлинности документа и цифровой подписи, а также для предупреждения мошенничества со стороны заверяющего в виде отказа его от подписи документа. Открытым ключом можно пользоваться только в том случае, если известны его подлинность и авторство, которые подтверждаются сертификатом. Поэтому во избежание подделки или внесения искажений, обмен и хранение открытых ключей должны осуществляться в защищенном виде. Для этого можно использовать секретный канал связи или в открытом канале связи средства электронной цифровой подписи, а при работе со средствами криптографической защиты необходимо контролировать целостность справочника открытых ключей.

Открытые ключи всех участников обмена информацией должны быть доступны всем для возможности проверки ЭЦП. То есть их можно размещать на серверах, передавать по радио, писать на заборах и публиковать в колонке частных объявлений в газете.

Естественно, говорить об этом с уверенностью можно только в том случае, если генерацию ключей производил сам владелец ключа либо (если он не располагает соответствующей техникой) удостоверяющий центр в его присутствии. В этой связи вызывает недоумение практика, распространенная в некоторых системах, когда организатор системы генерирует ключи заранее, а потом раздает пользователям.

На первом этапе для каждого абонента генерируют пару ключей — секретный и открытый, которые связаны между собой с помощью особого математического соотношения. Открытый ключ следует рассматривать как необходимый инструмент, по-

зволяющий определить автора подписи и достоверность электронного документа, но не позволяющий вычислить секретный ключ.

Возможны два варианта проведения этого этапа. Естественным представляется вариант, когда генерацию ключей абонент может осуществлять самостоятельно. Не исключено, однако, что в определенных ситуациях эту функцию целесообразно передать центру, который будет вырабатывать пары «секретный-открытый» ключ для абонентов и заниматься их распространением. Второй вариант имеет целый ряд преимуществ административного характера, однако обладает принципиальным недостатком — у абонента нет гарантии, что его личный секретный ключ уникален. Другими словами, можно сказать, что здесь все абоненты находятся «под колпаком» центра и он может подделать любую подпись.

Первый вариант заключается в том, что пользователь передает сам свой открытый ключ всем, с кем собирается вести переписку. По очевидным причинам он технически сложен (не со всеми можно встретиться лично, невозможно заранее предусмотреть всех адресатов).

Второй вариант заключается в создании центра сертификации (Certificate Authority). В качестве такого центра выбирают человека, которому все доверяют и с которым хотя бы один раз могут встретиться лично либо имеют надежный (т. е. не допускающий искажений/подделок) канал связи. После выбора такого лица все участники обмена генерируют свои пары ключей и, прихватив свой открытый ключ, выстраиваются в очередь к центру сертификации, который за умеренную плату удостоверяет личность пришедшего и подписывает его открытый ключ своим секретным ключом.

Кроме собственно открытого ключа, в блок подписываемых данных входят дополнительные сведения: имя владельца, другие идентифицирующие данные, сроки действия ключа, перечень информационных систем, в которых допустимо его использовать и др. Все это вместе (открытый ключ, блок данных и ЭЦП) называется сертификатом открытого ключа.

Владелец ключа получает на руки сертификат и открытый ключ центра. Теперь он просто счастлив — центр удостоверил принадлежность ключа ему (поэтому в Законе об ЭЦП данные центры именуются удостоверяющими центрами). Поскольку другие участники системы также получают вместе с сертификатом копию открытого ключа центра (получают лично), они могут удостовериться в принадлежности любого открытого ключа, не встречаясь лично с его владельцем, потому что теперь при установлении связи пользователи обмениваются не просто открытыми ключами, а сертификатами. Так, к почти строгому математическому механизму ЭЦП добавился организационный.

Таким образом, каждому пользователю, обладающему правом подписи, необходимо иметь лишь один секретный ключ и справочник регистрационных записей открытых ключей абонентов сети. Если у пользователя нет права подписи, но в процессе работы ему необходимо проверять подписи, проставленные под документами, он должен иметь лишь справочник открытых ключей. Для формирования справочника существует несколько возможностей. Например, список открытых ключей может формироваться в «центре» (выделенный пользователь, обладающий особыми полномочиями). «Центр» получает готовую регистрационную карточку открытого ключа абонента, формирует справочник открытых ключей, рассылает абонентам сети и контролирует его целостность и истинность.

Системы цифровой подписи организуются внутри инфраструктуры открытого ключа PKI (Public Key Infrastructure), которая поддерживается уполномоченным по сертификатам. Он отвечает за выдачу ключей и гарантирует подлинность сертификатов.

Базовые правила для каждой сети цифровой подписи должны быть тщательно проработаны. К примеру, необходимо определить, какой метод шифрования будет использоваться, кто будет выступать в роли уполномоченного по сертификатам.

Математические схемы, используемые в алгоритмах, реализующих цифровую подпись, основаны на однонаправленных функциях. Гипотеза о существовании односторонних функций является одним из результатов теории сложности и теории функций. Напомним, что односторонней называется функция, определенная (например) на множестве натуральных чисел и не требующая для вычисления своего значения больших вычислительных ресурсов. Но вычисление обратной функции (то есть по известному значению функции восстановить аргумент) оказывается невозможно теоретически или (в крайнем случае) вычислительно.

Строгого доказательства существования односторонних функций пока нет. Поэтому все используемые в настоящее время хэш-функции являются лишь кандидатами в односторонние функции, хотя и имеют достаточно хорошие свойства. Основными свойствами криптографически надежной хэш-функции являются:

- рассеивание;
- стойкость к коллизиям;
- необратимость.

Свойство рассеивания требует, чтобы минимальные изменения текста, подлежащего хэшированию, вызывали максимальные изменения значения хэш-функции. К таким изменениям относятся вставки, выбросы, перестановки и т. п.

Коллизией хэш-функции называется ситуация, когда два различных текста (вне зависимости от длины) могут иметь одинаковые хэш-функции. Значение хэш-функции всегда имеет фиксированную длину, а на длину исходного текста не накладывается никаких ограничений. Из этого следует, что коллизии существуют. Требование стойкости к коллизиям обозначает, что для криптографически надежной хэш-функции для заданного текста вычислительно невозможно найти другой текст, вызывающий коллизию. Иными словами, вероятность того, что значения хэш-функции двух различных документов совпадут, должна быть ничтожно мала.

Свойство необратимости заключается в том, что задача подбора документа, который обладал бы требуемым значением хэш-функции, вычислительно неразрешима. Для данной функции нельзя вычислить, какие два исходные сообщения могут генерировать одно и то же хэш-значение, поскольку хэш-значения двух 256-битных документов могут совпасть лишь в одном из 2256 (1077) случаев.

При подписании прежде всего документ «сжимают» до нескольких десятков или сотен байт с помощью хэш-функции. Здесь термин «сжатие» вовсе не аналогичен термину «архивирование». После архивирования информация может быть восстановлена. Значение же хэш-функции лишь только зависит от документа, но не позволяет восстановить сам документ.

Если к полученному хэш-значению применяется некоторое математическое преобразование (шифрование секретным ключом), то на выходе и получается цифровая подпись документа.

Размер собственно ЭЦП довольно велик, например, для ГОСТ Р 34.10-11.94 он равен 64-м байтам. После добавления служебной информации (порядка 50—200 байт в зависимости от реализации) эта величина существенно возрастает. Поскольку алгоритмы вычисления ЭЦП используют сложные алгебраические преобразования и являются сравнительно медленными, то для крупных центров обработки, где суточный объем электронных баз данных составляет величину порядка 50 000—60 000 шт., временные затраты на вычисление и проверку ЭЦП становятся значительными и заметно влияют на производительность системы в целом.

Процедура проверки подписи

Проверка подписи происходит в два этапа: вычисление хэш-функции документа и собственно математические вычисления, предусмотренные в данном алгоритме подписи, т. е. проверка того или иного соотношения, связывающего хэш-функцию документа, подпись под этим документом и открытый ключ абонента. Если требуемое соотношение выполнено, то подпись признается правильной, а сам документ — подлинным, в противоположном случае документ считается измененным, а подпись под ним — недействительной (рис. 4.36).

Проверяющий подпись должен располагать открытым ключом пользователя, поставившего подпись. Этот ключ должен быть аутентифицирован, то есть проверяющий должен быть полностью уверен, что данный открытый ключ принадлежит именно тому, кто выдает себя за его «хозяина». В случае, когда пользователи самостоятельно обмениваются ключами, эта уверенность может подкрепляться по телефону, личным контактом или любым другим способом. Когда же они работают в сети с выделенным центром, открытые ключи пользователей подписываются (сертифицируются) центром, и непосредственный контакт пользователей между собой (при передаче или подтверждении подлинности ключей) заменяется на контакт каждого из них с сертификационным центром.

Для разрешения споров между отправителем и получателем информации, связанных с возможностью искажения открытого ключа подписи, достоверная копия этого

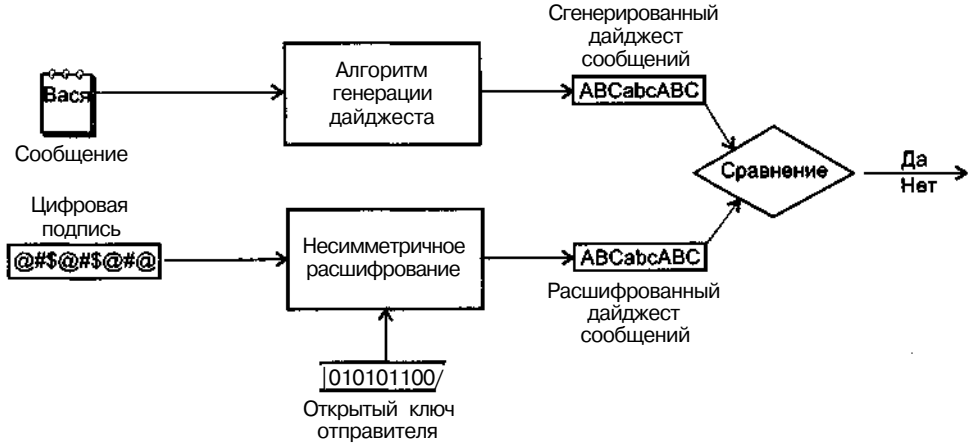


Рис. 4.36. Процедура проверки подписи

ключа может быть выдана третьей стороне (арбитру) и применена им при возникновении конфликта. Предъявляя контролеру открытый ключ — значение некоторой функции, вычисляемое с помощью секретного ключа, пользователь косвенным образом доказывает, что обладает секретным, но это еще не позволяет ему самому сменить свой номер в сети или выработать подпись под номером другого пользователя. Некоторые из них могут только проверять подписанные другими сообщения, другие (назовем их пользователями с правом подписи) могут как проверять, так и самостоятельно подписывать сообщения. Кроме того, бывают случаи, когда кто-либо может ставить свою цифровую подпись только в качестве второй подписи после подписи определенного пользователя (начальника, например); это не меняет существа дела.

Юридическая правомочность использования аналогов собственноручной подписи (разновидностью каковых и является ЭЦП) декларирована в Гражданском кодексе. Конечно же, наши респектабельные фирмы и банк заключили между собой соответствующие договоры, в которых стороны признают, что подписанные ЭЦП документы имеют такую же юридическую силу, что и документы на бумажном носителе, подписанные обычной подписью и заверенные печатью. В этом же договоре стороны определяют, при помощи какого именно программного обеспечения или аппаратуры будет формироваться ЭЦП, порядок его использования (организационные и технические меры безопасности) и, самое главное, порядок разрешения конфликтных ситуаций. Применительно к ЭЦП разновидностей конфликтных ситуаций не так много:

- отказ от авторства сообщения (я это не писал/не посылал);
- отказ от факта приема сообщения (я этого не получал);
- оспаривание времени приема/отправки сообщения.

Возникновение двух последних ситуаций предотвращается изначально продуманным протоколом обмена сообщениями между абонентами. Во-первых, к каждому сообщению перед подписанием прикрепляется отметка времени. Во-вторых, на каждое полученное сообщение получатель отправляет подписанное ЭЦП подтверждение о его приеме. Отправитель, в свою очередь, получив подтверждение, отправляет подписанную ЭЦП квитанцию. Таким образом, на каждый акт информационного обмена приходится 3 посылки, что, конечно же, избыточно, однако позволяет избежать упомянутых выше проблем (естественно, обе стороны ведут в течение оговоренного времени архивы принятых/посланных сообщений с ЭЦП).

Во многих случаях трехшаговое общение позволяет легко разрешить и ситуацию с отказом от авторства. Эта ситуация также должна быть предусмотрена в договоре и, во избежание недоразумений, должна быть расписана по шагам: как формируется комиссия (сроки, число членов с обеих сторон, необходимость привлечения независимых экспертов), порядок установки с эталонной копии средств проверки, формальные признаки, по которым осуществляется проверка, порядок оформления результатов. Не следует забывать и о сохранении копий сертификатов открытых ключей в удостоверяющем центре в течение необходимого срока, определяемого договором между участниками обмена. Естественно, срок хранения должен быть не менее исковой давности, определенной Гражданским кодексом или иными правовыми актами для данного вида договорных отношений.

Основными применяемыми на сегодняшний день алгоритмами, реализующими хэш-функции, являются MD2, MD4, MD5, SHA и его вариант SHA1, российский алго-

ритм, описываемый стандартом ГОСТ Р 34.11-94. Наиболее часто используются MD5, SHA1 и 34.11 в России. Длина значения **хэш-функции** различна. Типичная длина составляет 16—32байта.

Существует много математических схем подписи, наиболее известные из которых:

- RSA (R.L.Rivest, A.Shamir, L.Adleman) назван по первым буквам фамилий авторов;
- OSS (H.Ong, C.P.Schnorr, A.Shamir);
- Эль-Гамаля (T.ElGamal);
- Рабина (M.Rabin);
- Шнорра (C. P. Schnorr);
- Окамото-Сарайси (T.Okamoto, A.Shiraishi);
- Мацумото — Имаи (T.Matsumoto, H.Imai);
- схемы с использованием эллиптических кривых и др.

В схемах RSA, Рабина, Эль-Гамаля и. Шнорра трудность подделки подписи обусловлена вычислительной сложностью задач факторизации или дискретного логарифмирования. Среди схем, предложенных отечественными учеными, можно отметить оригинальную схему А. А. Грушо (1992 г.). Ее однонаправленная функция, в отличие от перечисленных выше, основана не на сложности теоретико-числовых задач, а на сложности решения систем нелинейных булевых уравнений. На базе перечисленных выше схем подписи созданы стандарты на ЭЦП. Стандарт — это достаточно подробное описание алгоритмов, по которым вычисляется и проверяется подпись.

В принятых стандартах на цифровую подпись США и России (DSS — Digital Signature Standard, ГОСТы Р 34.10-94 и Р 34.11-94) используются специально созданные алгоритмы. В основу этих алгоритмов положены схемы Эль-Гамаля и Шнорра.

Федеральный стандарт цифровой подписи DSS, который был впервые опубликован в 1991 году в США, описывает систему цифровой подписи DSA (Digital Signature Algorithm). Этот алгоритм разработан Агентством Национальной Безопасности США и принят в качестве стандарта цифровой подписи Национальным Институтом Стандартов и Технологии. Алгоритм использует метод **шифрования** с открытым ключом и является основой всей электронной коммерции, обеспечивая конфиденциальность и достоверность передаваемых по Internet данных. Длина подписи в системе DSA составляет 320 бит. Надежность всего стандарта основана на практической неразрешимости задачи вычисления дискретного логарифма. Однако, к сожалению, сегодня этот алгоритм уже не имеет достаточного временного запаса по нераскрываемости (10—20 лет). Прореха скрывается в несовершенстве подпрограммы генерации псевдослучайных чисел. Вместо того чтобы вычислять разные цифры с равной вероятностью, она выбирает числа из некоторого диапазона. Этот недостаток цифровой подписи заметно облегчает ее взлом с использованием современных суперкомпьютеров.

В России «Закон об электронной цифровой подписи» принят Государственной думой 21 ноября 2001 года. В нем установлена права и обязанности обладателя цифровой подписи, указаны сертификаты ключа, выдаваемые удостоверяющим центром, определены состав сведений, содержащихся в сертификате ключа, срок и порядок его хранения и т. д.

У нас в стране выработка и проверка электронной цифровой подписи производятся на основе отечественного алгоритма **криптопреобразования** ГОСТ 28147-89. Данная

процедура предусматривает использование двух различных ключей криптографического алгоритма отечественного стандарта. Этими ключами одновременно владеет только отправитель, который и подписывает сообщение. Кроме того, предполагается наличие двух независимых центров доверия (Центр 1 и Центр 2), которым доверяют все пользователи данной системы электронной цифровой подписи.

Кроме того, в России приняты стандарты: ГОСТ Р 34.10-94 «Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма» и ГОСТ Р 34.11-94 «Функция хэширования». В основу ГОСТ Р 34.10-94 положена однонаправленная функция, основанная на дискретном возведении в степень. Можно быть вполне уверенным, что алгоритм из стандарта ГОСТ Р 34.10-94 обладает высокой криптографической стойкостью.

Пользователи Internet используют в качестве основы своей системы ЭЦП известный пакет программ PGP, созданный под руководством Филиппа Зиммерманна. К основным преимуществам данного пакета, выделяющим его среди других аналогичных продуктов, относятся:

- открытость;
- стойкость;
- бесплатность;
- G поддержка различных моделей распределения ключей;
- удобство программного интерфейса.

Открытость основана на том, что доступен исходный код всех версий программ PGP. Любой эксперт может убедиться, что в программе криптоалгоритмы реализованы эффективно. Для повышения стойкости криптоалгоритма применяются ключи достаточно большой длины. Пакет поддерживает как централизованную модель (через серверы ключей), так и децентрализованную модель (через сеть доверия) распределения ключей.

Однако, несмотря на то что пакет свободно распространяется по сетям, это не означает, что его можно легко и доверительно использовать — существует патентное законодательство. Кроме того, в этих программах обнаружено несколько закладок (в частности, против систем, построенных на основе пакета программ PGP), при помощи которых были подделаны электронные документы.

В марте 2001 года два чешских криптолога объявили, что ими была обнаружена «дыра» в самой популярной программе шифрования электронных посланий — PGP. Ошибку обнаружили при изучении надежности электронной подписи в открытом формате OpenPGP, широко используемом сейчас для присылки сообщений.

Это уже второй случай обнаружения в PGP «дыры» для несанкционированного доступа к зашифрованным сообщениям. Предполагается, однако, что на этот раз дело обстоит несколько серьезнее, чем в случае с возможностью добавлять к открытому ключу дополнительный ключ ADK (Additional Decryption Key) и таким образом дешифровать данные. Как известно, чтобы воспользоваться этой программной ошибкой, необходимо сначала получить доступ к передаваемому сообщения компьютеру либо напрямую, либо через Internet. Обнаруженное уязвимое место в программе не дает возможности взлома кода, который до сих пор считается достаточно надежным, но открывает пути доступа, позволяющие мошеннику украсть у пользователя один из ключей.

Подчеркнем, что под стандартом на электронную подпись понимается только стандарт на криптографический алгоритм. Многие существенные детали в стандарте не оговорены (например, способ распространения открытых ключей, способ генерации псевдослучайных чисел и др.). Это, вообще говоря, может привести к тому, что разные средства, осуществляющие функции ЭЦП (каждое из которых соответствует стандарту!), окажутся несовместимыми между собой.

Новый отечественный стандарт на ЭЦП

В 2001 году на конференции, проводившейся Ассоциацией документальной электросвязи и представителями ФАПСИ, было официально объявлено об утверждении нового стандарта на электронную цифровую подпись. Этот стандарт, основанный на методе эллиптических кривых, вступает в силу с 1 июля 2002 года. Он придет на смену тому стандарту, который используется сейчас и который мы рассматривали выше. Новый стандарт будет иметь тот же номер, что и старый, за исключением того, что изменятся лишь цифры, обозначающие год.

Все ранее сертифицированные криптографические системы, использующие старый стандарт, сохранят свои сертификаты до конца срока их действия. Для всех новых или вновь сертифицируемых систем новый стандарт будет обязательным.

Ввод в действие нового стандарта связан с тем, что по словам гендиректора ФАПСИ, действующий стандарт уже к 2003 году не будет обеспечивать достаточный уровень защиты. И хотя для подделки одной ЭЦП, соответствующей старому ГОСТу, сегодня требуется около 10 лет работы 10 000 компьютеров, он же и существенно увеличивает длину обрабатываемых сообщений (в российском алгоритме используются очень длинные ключи).

Проблему **криптостойкости** существующего стандарта можно было бы решить, увеличив длину шифровального ключа подписи, однако это приведет к неоправданным затратам и увеличению длительности обработки. Поэтому в новой редакции стандарта и используется математика эллиптических кривых.

Сегодня работа стандартов ЭЦП основана, в основном, на:

- классической математике;
- эллиптических кривых, использующих теорию алгебраических чисел.

Если первый подход уже давно известен, то второй метод подразумевает более короткий ключ, при этом процедуры обоснования его надежности сложнее, поскольку экспертов в области эллиптических кривых гораздо меньше, чем специалистов по теории чисел. Ключи в алгоритме с использованием эллиптических кривых могут быть созданы в 100 раз быстрее и занимают гораздо меньше места, чем ключи в алгоритме RSA.

Совсем недавно для оценки криптостойкости алгоритма, основанного на методе эллиптических кривых, были предприняты попытки взлома шифра с 97-битным ключом. Эта задача, поставленная Французским национальным институтом информатики (INRIA), была решена командой энтузиастов под руководством ирландского математика Роберта Харли (Robert Harley). Для этого потребовались 40-дневные объединенные усилия 195 добровольцев из 20 стран и 740 независимых компьютеров. По словам Роберта Харли, решить задачу шифрования с 97-битным дискретным алгоритмом на

основе эллиптических кривых труднее, чем взломать 512-битный несимметричный шифр RSA, который сегодня является промышленным стандартом.

Несколько позднее канадской компанией Certicom, занимающейся вопросами шифрования, которая хотела привлечь исследователей к тестированию уровня защиты, обеспечиваемого алгоритмом ECC (Elliptic Curve Cryptography), было инициировано исследование, посвященное анализу уже 109-разрядного ключа. Эта задача, получившая известность под кодовым наименованием ECC2K. 108, была решена с помощью распределенной сети, включающей большое число компьютеров. В ее решении приняли участие 1300 человек из 40 стран, перебиравшие всевозможные комбинации ключей до тех пор, пока не был обнаружен искомый. Исходное тестовое сообщение было закодировано с помощью метода эллиптических кривых.

В своем проекте Certicom использовала свободно распространяемое программное обеспечение, которое Роберт Харли разработал для вычисления более 215 точек на эллиптической кривой, относящейся к классу кривых Коблитца. Данные о 2 млн «выделенных» точек были посланы на сервер AlphaServer в INRIA, где участники могли в реальном времени наблюдать за поиском ключа. Для взлома алгоритма использовались 9500 компьютеров в Internet. По данным INRIA, две трети вычислений пришлось на долю рабочих станций с операционной системой Unix, а одна треть — на компьютеры с Windows.

На решение такой задачи на одном компьютере с процессором Pentium И/450 МГц потребовалось бы примерно 500 лет. «Объем вычислений, проделанных нами, больше, чем нужно для взлома системы, защищенной открытым ключом наподобие RSA длиной как минимум 600 разрядов», — отметил Эрьен Ленстра, вице-президент по технологиям подразделения Citibank в Нью-Йорке, который также принимал участие в проекте. И это с учетом того, что компания Certicom выбрала кривую, отличающуюся свойствами, упрощающими задачу взлома кода, и была проделана примерно десятая часть всех вычислений, которые в обычных условиях должны потребоваться для взлома 109-разрядного ключа при шифровании по кривой. Проведенный проект показал относительную уязвимость некоторых кривых с особыми свойствами и подтвердил тот факт, что произвольные кривые лучше подходят для оптимальной защиты.

Остановимся вкратце на рассмотрении метода эллиптических кривых, использованного в новом стандарте на электронную цифровую подпись. Эллиптическая кривая описывается математическим уравнением вида:

$$y2 = x3 + ax + \mathbf{b},$$

где все вычисления выполняются по модулю выбранного просто числа p и 4a3 + 27b2 = 0.

Этот случай называется нечетным, т. к. модуль p берется для некоторого числа нечетных значений p. Четный случай аналогичен, но вычисления при этом ведутся в конечном поле GF(2m) для некоторого целого числа т.

Проблему дискретного логарифма DLP (Discrete Logarithm Problem) кратко можно сформулировать так: «По заданному простому числу p, основанию g и значению gx(mod p) найти значение x». Причем проблема может быть сформулирована в ограниченной области.

Полезное для криптографии свойство эллиптических кривых состоит в том, что если взять две различных точки на кривой (рис. 4.37), то соединяющая их хорда пересечет кривую в третьей точке (так как мы имеем кубическую кривую). Зеркально отразив эту точку по оси X, мы получим еще одну точку на кривой (так как кривая симметрична относительно оси X). Это позволяет точно определить форму кривой. Если мы обозначим две первоначальные точки P и Q, то получим последнюю (отраженную) точку P+Q. Представленное «сложение» удовлетворяет всем известным алгебраическим правилам для целых чисел, позволяя определить единственную дополнительную точку, которая называется бесконечно удаленной точкой и выполняет роль нуля (начала отсчета) для целых чисел.

Другими словами, можно определить форму кривой по заданным точкам (плюс бесконечно удаленной точке), что является обычным алгебраическим действием. Выражаясь математическими терминами, можно определить конечную абелеву группу (абстрактную группу с коммутативной бинарной операцией) на точках кривой, где нулем будет бесконечно удаленная точка. В частности, если точки P и Q совпадут, то можно вычислить P+P. Развивая эту идею, можно определить **kP** для любого целого числа k, и, следовательно, определить значение P и значение наименьшего целого числа k, такого что kP = F, где F — бесконечно удаленная точка. Теперь можно сформулировать Проблему дискретного логарифма эллиптической кривой (Elliptic Curve Discrete Logarithm Problem, ECDLP), на которой основана рассматриваемая система:

- Для эллиптических кривых и базовых точек решение уравнений типа «Даны базовая точка P и расположенная на кривой точка kP; найти значение k.» представляет весьма и весьма сложную задачу. С точки же зрения криптографии на основе эллиптических кривых имеется возможность определить новую криптографическую систему (любая стандартная система, основанная на проблеме дискретного логарифма, аналогична системе основанной на ECDLP). Например, эллиптическая кривая DSA (ECDSA) уже стандартизована (ANSI X9.62), и на ее базе можно реализовать протокол открытого обмена ключами Diffie-Hellman.
- При определении системы эллиптической кривой требуются сама кривая и базовая точка P. Эти элементы не являются тайной и могут быть одинаковыми для всех пользователей системы. Для данной кривой и точки несложно сгенерировать открытые и частные ключи для пользователей (частный ключ представляет просто случайное целое число k, а открытый ключ — точку **kP** на кривой). Однако чрезвычайно трудно создать подходящую кривую и точку. Главное — подсчитать количество точек на кривой. Для этого необходимо выбрать подходящую базовую точку P, координаты которой должны иметь достаточно большое значение, чтобы гарантировать трудность взлома ECDLP. Но координаты точки P должны делиться на количество точек на кривой (точки вместе с бесконечно удаленной точкой образуют конечную группу). И весьма веро-

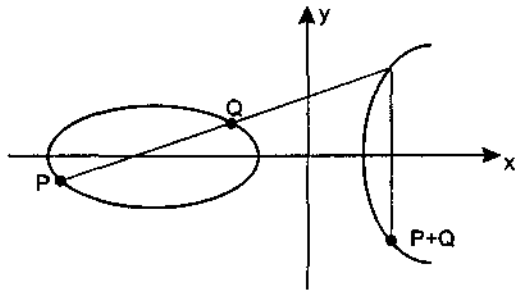


Рис 4 37 Свойства эллиптических кривых

ятно, что, найдя число точек на кривой, мы не сможем найти базовую точку. Существуют и другие ограничения, которые необходимо учесть при построении кривых.

Подводя итог вышеизложенному, можно утверждать, что создание кривых — задача непростая. Пользователи могут применять «стандартные» кривые с помощью специального программного обеспечения, либо создавать собственные кривые, что занимает, к сожалению, очень много времени.

Системы на основе эллиптической кривой используют ключи малых размеров. Это значительно снижает требования к вычислительным мощностям по сравнению с требованиями систем на основе RSA. Как это влияет на скорость обработки, показывает табл. 4.10. В ней представлены сравнительные характеристики алгоритмов RSA и ECDSA (нечетный случай) при создании и проверке цифровых подписей. Оба алгоритма тестировали на параллельных процессорах Motorola 56303 DSP (66 МГц). При этом функция проверки подписи RSA использует e = 65 537.

Таблица 4.10. Сравнительные характеристики алгоритмов RSA и ECDSA (нечетный случай) при создании и проверки цифровой подписи

Алгоритм (длина ключа, бит)	Время выполнения, мс	
	Создание подписи	Проверка подписи
RSA (1024)	25	< 2
ECDSA (160)	32	33
RSA (2048)	120	5
ECDSA (216)	68	70

Как видно из табл. 4.10, при увеличении размеров ключа создание подписей с помощью ECDSA производится значительно быстрее, чем в системах RSA. Это различие в еще большей степени проявляется для однопроцессорных систем. С другой стороны, проверка подписи с помощью ECDSA, делается намного медленнее, чем эта же процедура в системах RSA и опять же различие усиливается для систем с одним процессором.

Обработка ECDSA может несколько ускориться в «четном» случае. Мощность процессора, затраченная на проверку подписи, при использовании, скажем, ECDSA может замедлить выполнение других приложений в системе. Множество систем имеют много удаленных устройств, соединенных *с* центральным сервером, и время, затраченное удаленным устройством для создания подписи (несколько секунд), не влияет на производительность системы в целом, но сервер должен также и подтверждать подписи, причем очень быстро. В некоторых случаях системы RSA (даже использующие большие ключи) возможно, будут более приемлемы, чем криптосистемы на основе эллиптической кривой.Тем не менее, криптосистемы на основе эллиптической кривой получают все большее распространение скорее как альтернатива, а не замена систем RSA, поскольку системы ECDLP имеют некоторые преимущества, особенно при использовании в устройствах с маломощными процессорами и/или маленькой памятью. Типичные области применения алгоритма на основе эллиптической кривой:

- m-commerce (мобильная торговля) (например, WAP, сотовые телефоны, карманные компьютеры);
- смарт-карты (например, EMV);

- e-commerce (электронная торговля) и банковские операции (например, SET);
- Internet-приложения (например, SSL).

Из-за очевидной трудности взлома алгоритм ECDLP можно применять для высоко защищенных систем, обеспечивая достаточно высокий уровень безопасности. Как уже говорилось выше, в рассматриваемом алгоритме используются ключи значительно меньшего размера, чем, например, в алгоритмах RSA или DSA. В табл. 4.11 сравниваются приблизительные параметры эллиптических систем и RSA, обеспечивающих одинаковую стойкость шифра, которая рассчитывается на основе современных методов решения ECDLP и факторинга (поиска делителей) для больших целых чисел.

Таблица 4.11. Параметры эллиптических систем и RSA, обеспечивающих одинаковую стойкость шифра

Длина ключа, бит	
Система на основе эллиптической кривой (базовая точка P)	RSA (длина модуля n)
106	512
132	768
160	1024
224	2048

Из табл.4.11 видно, что, используя эллиптические кривые, можно строить хорошо защищенные системы с ключами явно меньших размеров по сравнению с аналогичными «традиционными» системами типа RSA или DSA. В частности, такие системы менее требовательны к вычислительной мощности и объему памяти оборудования и потому удобны, например, для смарт-карт или портативных телефонов.

Разумеется, есть и проблемы, ограничивающие повсеместное распространение криптографических систем на основе эллиптических кривых.

Главная проблема состоит в том, что истинная сложность ECDLP еще не осознана полностью. Недавнее исследование показало, что некоторые эллиптические кривые, использовавшиеся для отработки алгоритмов шифрования, фактически не подходят для таких операций. Например, если координаты базовой точки P равны положению p, то ECDLP имеет простое решение. Такие кривые являются «аномальными» кривыми. Существуют, однако, и некоторые другие проблемы:

- реальная безопасность таких систем все еще недостаточно исследована;
- трудность генерации подходящих кривых;
- несовместимость с другими системами;
- относительно медленная проверка цифровой подписи.

Системами электронного документооборота с использованием ЭЦП оснащены администрация президента и представительства президента в федеральных округах. Сертифицированные средства используют Внешторгбанк (система «Верба»), Сбербанк, Министерство по налогам и сборам, Пенсионный фонд, внедрена система ЭЦП в аппарате правительства РФ.

Сертификацией средств электронно-цифровой подписи занимается ФАПСИ. Сегодня существуют две сертифицированные системы — «Криптон» фирмы «Анкад» и

«Крипто-про CSP» компании «Крипто-про». Действие сертификата ФАПСИ на систему «Верба» производства МО ПНИЭИ фактически закончилось.

По Указу Президента, применение сертифицированных ФАПСИ средств ЭЦП сегодня обязательно для государственных организаций, однако в действительности эта норма легко обойти (например, применение ЭЦП можно назвать «защитой информации»). Так, не сертифицированные в ФАПСИ средства применяются в ФСБ, МИДе и отчасти в Центробанке. Однако по новому закону использование сертифицированных ФАПСИ алгоритмов электронно-цифровой подписи в госорганах планируется сделать строго обязательным.

ГЛАВА 5. КОМПЬЮТЕРНАЯ СТЕГАНОГРАФИЯ

Как известно, цель криптографии (шифрования) состоит в сокрытии содержания секретных сообщений. Стеганография идет принципиально дальше. Ее задача — скрыть от непосвященных сам факт существования сообщений. Такие скрытые сообщения могут включаться в различные внешне безобидные данные, вместе с ними храниться и передаваться без всяких подозрений со стороны. Если разработчики криптографических алгоритмов исходят из предположения, что потенциальный противник будет делать что угодно для дешифровки сообщения, то разработчик стеганографического алгоритма озабочен тем, как не дать противнику обнаружить существование самого сообщения, содержащего тайну.

Стеганография имеет многовековую историю и по возрасту существенно старше криптографии. Само слово «стеганография» в переводе с греческого буквально означает «тайнопись» (steganos — секрет, тайна; graphy — запись). В основе искусства скрытого письма лежит попытка скрыть само существование секретного сообщения, а потому его приемы заслуживают самого широкого употребления. Для тайнописи могут быть использованы: «подкладочное письмо», когда запись сокрыта какой-либо защитной оболочкой, «хоббийное кодирование», с использованием кроссвордов, музыкальных нот и шахматных партий, «жаргонные шифры», в которых вроде бы невинные слова имеют совершенно другой смысл. К ней относится огромное множество секретных средств связи и передачи информации, таких, как невидимые чернила, микрофотоснимки (микроточки), условное расположение знаков, незначительные различия в написании рукописных символов, маленькие проколы определенных напечатанных символов и множество других способов по скрытию истинного смысла тайного сообщения в открытой переписке, тайные каналы и средства связи на плавающих частотах, и т. д. Хорошо известны различные способы скрытого письма между строк обычного не защищаемого письма: от применения молока до использования сложных химических реакций с последующей обработкой при чтении.

Первые следы стеганографических методов передачи информации теряются в глубокой древности. История стеганографии — это история развития самого человечества. Рассмотрим кратко, как происходило становление стеганографии.

Местом зарождения стеганографии многие называют Египет, хотя первыми «стеганографическими сообщениями» можно назвать и наскальные рисунки древних людей.

Первое упоминание в литературе о стеганографических методах приписывается Геродоту, который еще в 474 году до н.э. описал случай с тираном Гистием. Последний, запертый указом персидского царя Дария в Сузах, захотел пообщаться с одним из своих родственников за пределами Суз. Чтобы его послание не попало в чужие руки, Гистий поступил очень остроумно — он обрил голову раба, вытатуировал письмо на коже головы, подождал, пока снова отрастут волосы, и отправил невольника в Милет под благовидным предлогом. Там раба снова побрили и прочитали послание. Для нашего времени этот способ, конечно, весьма сомнительный — и ждать пока волосы отрастут долго, и гонец получается одноразовый (больше одного письма на голове не вытатуируешь, а свести татуировку и сегодня проблема, не то, что в V веке до н.э.) — но важен принцип.

Геродотом описан еще один, чуть менее известный и немного менее зрелищный случай, который относят к тем же временам. Как утверждает Геродот, Демарт передавал послания, придерживаясь тех же правил, что и Гистий, т.е. скрывал сам факт передачи сообщения. Другое дело, что Демарту хватило сообразительности немного ускорить процесс подготовки посланий — он соскабливал с восковых дощечек воск, царапал свои секретные послания прямо на дереве, а позже покрывал дощечки воском заново.

В Китае письма писали на полосках шелка. Поэтому для сокрытия сообщений полоски с текстом письма сворачивались в шарики, покрывались воском и затем глотались посыльными. Как эти послания доставали, мы описывать не будем.

Темное средневековье породило не только инквизицию: усиление слежки привело к развитию как криптографии, так и стеганографии. Именно в средние века впервые было применено совместное использование шифров и стеганографических методов.

В XV веке монах Тритемиус (1462—1516), занимавшийся криптографией и стеганографией, описал много различных методов скрытой передачи сообщений. Позднее, в 1499 году, эти записи были объединены в книгу «Steganographia», которую в настоящее время знающие латынь могут прочитать в сети Internet.

XVII — XVIII века известны как эра «черных кабинетов» — специальных государственных органов по перехвату, перлюстрации и дешифрованию переписки. В штат «черных кабинетов», помимо криптографов и дешифровальщиков, входили и другие специалисты, в том числе и химики. Наличие специалистов-химиков было необходимо из-за активного использования так называемых невидимых чернил. Примером может служить любопытный исторический эпизод: восставшими дворянами в Бордо был арестован францисканский монах Берто, являвшийся агентом кардинала Мазарини. Восставшие разрешили Берто написать письмо знакомому священнику в город Блэй. Однако в конце этого письма религиозного содержания монах сделал приписку, на которую никто не обратил внимание: «Посылаю Вам глазную мазь; натрите ею глаза и Вы будете лучше видеть». Так он сумел переслать не только скрытое сообщение, но и указал способ его обнаружения. В результате монах Берто был спасен.

Стеганографические методы активно использовались американцами в годы гражданской войны между южанами и северянами. Так, в 1779 году два агента северян Сэмюэль Вудхулл и Роберт Тоунсенд передавали информацию Джорджу Вашингтону, используя специальные чернила.

Еще древние римляне писали между строк невидимыми чернилами, в качестве которых использовались фруктовые соки, моча, молоко и некоторые другие натуральные вещества. Их опыт не был забыт. Различные симпатические чернила использовали и русские революционеры в начале XX века. Симпатические чернила или, с успехом выполняющее их роль, обычное молоко — один из самых распространенных стеганографических методов. Большинство читателей, очевидно, помнит рассказы о Ленине, писавшем свои труды в местах не столь отдаленных. Многие книги были написаны им молоком между строк. Чернильницей Ильичу служил хлебный мякиш — при малейшем подозрительном звуке будущий вождь мирового пролетариата мигом съедал свои стеганографические приспособления. Позднее исписанные молоком листы передавались на волю, а там нагревались над лампой и переписывались товарищами по партии. Впрочем, царская охранка тоже знала об этом методе (в ее архиве хранится документ, в котором описан способ использования симпатических чернил и приведен текст перехваченного тайного сообщения революционеров).

К середине 20-го века стеганография достигла значительных успехов, чему не мало поспособствовали Первая и Вторая мировые войны. Особенных успехов добились немцы, которые во время Второй мировой войны широко применяли «микроточки», представлявшие из себя микрофотографии размером с обычную типографскую точку. При увеличении «микроточка» давала четкое изображение печатной страницы стандартного размера. Такая точка или несколько точек вклеивались в обыкновенное письмо, и, помимо сложности обнаружения, обладали способностью передавать большие объемы информации, включая чертежи и рисунки.

Сам метод был придуман намного раньше, почти сразу после изобретения принципа фотографической печати. Микроточки появились сразу же после изобретения Дагером фотографического процесса, и впервые в военном деле были использованы во времена франко-прусской войны (в 1870 году), но широкого применения до Второй мировой войны этот метод не имел. Но во время Второй мировой войны этот метод претерпел второе рождение и успех его был весьма заметным. Американцы, впечатленные достижениями своего противника в стеганографии, после войны запретили даже такие относительно невинные операции, как пересылку посредством почты записей шахматных партий, инструкций по вязанию (!) и даже детских рисунков, как наиболее простых с точки зрения стеганографа объектов для встраивания шпионских сообщений. Сегодня, конечно, подобные запреты неактуальны: любой шпион может послать e-mail, предварительно зашифровав его с помощью DES, к примеру.

Тем не менее, на практике, стеганография давно и широко использовалась разведками всех стран. Успех разведчика, да и сама его жизнь, зависят от умения остаться незамеченным. Поэтому шифр — это язык разведчиков всех стран. Именно они обычно вынуждены вести свои разговоры «шепотом». Они используют коды, имеющие вид обычных открытых текстов, невидимые чернила, послания микроскопически малых размеров, т. е. стеганографические методы, которые скрывают сам факт отправки какого-либо сообщения.

После нападения Японии Соединенные Штаты создали орган цензуры, насчитывающий около 15 тысяч сотрудников, которые проверяли ежедневно до миллиона писем, прослушивали бесчисленное множество телефонных разговоров, просматривали кинофильмы, газеты, журналы.

Чтобы перекрыть максимальное число стеганографических каналов связи, американская цензура категорически запретила отправление по почте целого ряда сообщений. Были отменены шахматные матчи по переписке. Из писем вымарывались кроссворды, т. к. у цензоров не хватало времени решать их, чтобы проверить, не содержат ли они тайные послания. Не разрешалось посылать по почте табели успеваемости учащихся, вырезки из газет, детские рисунки, инструкции по вязанию и шитью. Одно письмо с инструкциями по вязанию было задержано до тех пор, пока цензор не связал по ним свитер, чтобы проверить, не содержат ли они какой-либо скрытой информации.

Распространение стеганографии во время войны и тотальная шпиономания вызвали появление многих цензурных ограничений, которые сегодня могут вызвать лишь улыбку. Запрещалось посылать телеграммы с указанием доставить определенный сорт цветов к определенной дате, а впоследствии американским и английским правительствами были запрещены вообще все международные телеграммы, касающиеся доставки и заказа цветов. Как обстояли дела с международной почтой в СССР, рассказывать, думаю, не надо.

Ориентирующими примерами данных методик (оставив в стороне возможности, даваемые электроникой) могут служить:

- ❑ запись наколом букв в конкретном месте некой книги или газеты (концы слов отмечаются при этом наколом между буквами);
- G сообщение каких-то данных (набор товаров, оптовые цены) в определенном порядке;
- ❑ письмо посредством узелков, где каждая из букв кодируется размером в сантиметрах (А-1 см, Б-2 см...) или в диаметрах мизинца и отмечается отдельным узелком на нитке или на обвязывающем сверток шпагате; читают текст, наматывая нитку на палец;
- ❑ запись на боковой поверхности колоды карт, подобранных в конкретном порядке (колода после этого тасуется);
- ❑ записи на оборотной стороне этикеток флаконов, банок или бутылок;
- ❑ текст под наклеенной почтовой маркой;
- ❑ запись на внутренней поверхности спичечной коробки, которая для этого разламывается, а после склеивается по новой;
- ❑ запись внутри вареного яйца (берут смесь квасцов, чернил и уксуса, записывают ею то, что необходимо на скорлупе обычного яйца, которое потом выдерживают в крепком рассоле или уксусе, чтобы стравить следы с его поверхности; яйцо затем варят вкрутую, причем весь текст оказывается сверху белка под скорлупой);
- ❑ использование «испорченной» пишущей машинки, в которой некоторые буквы ставятся выше или ниже строки (учитывают здесь порядок и число этих букв, а также промежутки их появления; в коде возможен вариант азбуки Морзе);
- ❑ записи от руки нот в нотной тетради (ноты имеют здесь значение по азбуке Морзе или иному коду);
- О записи в виде кардиограммы или же графика некого технологического процесса (здесь, при использовании азбуки Морзе, пики повыше означают, скажем, точки, а те, что ниже, — тире, черточки между зубцами сообщают о разделе между буквами, разрывы линии фиксируют конец слова);

- записи лишь в вертикальных столбцах цельно заполненного кроссворда (горизонтальные строки при этом заполняются произвольно, само же сообщение может быть либо прямым, либо кодированным);
- записи по трафарету, при этом на лист почтовой бумаги накладывают трафарет с вырезанными в нем окошками, следуя по которым и вписывают истинное сообщение; все остальное пространство здесь тщательно заполняется «пустым» содержанием, так, впрочем, чтобы слова подлинной информации четко входили в текст ясного маскировочного послания;
- шифр «Аве Мария», в кодовом варианте которого каждому слову, а порой и фразе, ставятся в соответствие несколько слов явной религиозной тематики, так что передаваемое сообщение выглядит как специфический текст духовного содержания.

Развитие компьютерной технологии и средств коммуникации сделали бесполезными подобные ограничения. Сегодня каждый может воспользоваться теми преимуществами, которые дает стеганография как в области скрытой передачи информации, что особенно полезно в странах, где существует запрет на стойкие средства криптографии, так и в области защиты авторских прав.

Сильным толчком к развитию стеганографии послужило то, что в большинстве стран на криптографию накладываются определенные ограничения: так, например, требуется передача ключей от используемых систем шифрования государству. Обязательна также регистрация и лицензирование криптографических систем независимо от того, являются они аппаратными или программными средствами. Стеганография — это тот метод, который не попадает под действие указанных ограничений, являясь при этом эффективным способом сокрытия данных.

Возродилась старая идея использования микроточки, выполняемая теперь с помощью компьютера. Кто заподозрит, что в электронном документе, отправленном, скажем, через Internet, одна из точек вовсе не точка, а скрытое сообщение? А вот получатель документа с помощью специальных программных средств как бы увеличит компьютерную микроточку и сможет прочесть скрытую информацию.

Скрытие сообщений с помощью микроточек эффективно, если противник не знает, как именно это сделано. Поэтому разработка программного обеспечения для автоматического «наклеивания» и «увеличения» микроточек выполняется по индивидуальным заказам.

В марте 2000 года 17-летняя американская школьница Вивиана Риска создала алгоритм, который может «прятать» сообщение в генную последовательность молекулы ДНК. На конкурсе молодых ученых компании Intel Science Talent Search (этот смотр молодых талантов называют «Нобелевской премией для молодежи») она продемонстрировала технологию внедрения компьютерных сообщений в генную последовательность молекулы ДНК. Пробным сообщением, шифровку которого девушка продемонстрировала жюри конкурса, была фраза «Вторжение 6-го июля: Нормандия».

Еще одной областью использования стеганографии является защита авторского права от пиратства. На компьютерные графические изображения наносится специальная метка, которая остается невидимой для глаз, но распознается специальным программным обеспечением. Такое программное обеспечение уже используется в компьютерных версиях некоторых журналов. Данное направление стеганографии предназначено не только для обработки изображений, но и для файлов с аудио- и видеоинформацией и призвано обеспечить защиту интеллектуальной собственности.

За время своего существования человечество изобрело большое число способов секретного письма, многие из них были известны еще в древности. Как мы уже говорили, в некоторых способах тайного письма используются физические особенности носителей информации. Это очень интересная тема, однако она является предметом изучения физики и химии, и никакого отношения к теории информации не имеет. Для массового практического применения гораздо больший интерес представляют методы защиты данных, которые опираются исключительно на свойства самих данных и никак не связаны с особенностями их физического представления. Образно говоря, при использовании методов данного типа барьер между собственно сообщением и злоумышленником, желающим его прочитать или исказить, возводится исключительно из самой информации. Речь в дальнейшем пойдет только о таких способах защиты. Мы остановимся на рассмотрении современного и сравнительно нового направления этой сферы человеческой деятельности — компьютерной стеганографии.

Принципы построения компьютерной стеганографии

Стеганография занимает свою нишу в обеспечении безопасности: она не заменяет, а дополняет криптографию, защищая информацию от злоумышленников. Сокрытие сообщения методами стеганографии значительно снижает вероятность обнаружения самого факта передачи сообщения. А если это сообщение к тому же зашифровано, то оно имеет еще один, дополнительный, уровень защиты.

Стеганография бывает полезна, когда необходимо не просто передать секретное сообщение, а секретно передать секретное сообщение, то есть скрыть сам факт передачи секретного сообщения. Такой способ ведения тайной коммуникации, однако, имеет ряд недостатков:

- трудно обосновать его стойкость — вдруг злоумышленникам станет известен способ «подмешивания» секретных данных к «болванке» — массиву открытых данных;
- при его использовании объем передаваемых или хранимых данных может увеличиваться, что отрицательно сказывается на производительности систем их обработки.

В зависимости от способа засекречивания передаваемых сообщений, а именно прячется ли секретное сообщение или оно просто делается недоступным для всех, кроме получателя, можно выделить два класса засекречивания данных — стеганографию и шифрование.

Если рассматривать информацию отдельно от ее материального представления, а именно так мы и будем ее рассматривать, то возникает вопрос — где же информацию можно спрятать? Ответ однозначен: только в еще большем массиве информации — как иголку в стоге сена. В этом и заключается принцип действия стеганографии, т.е. стеганография предполагает, что передаваемый текст «растворяется» в сообщении большего размера с совершенно «посторонним» смыслом. Но если взять и извлечь из него некоторые символы по определенному закону,

например, — каждый второй, третий, и т.д., то получим вполне конкретное тайное сообщение.

Компьютерная стеганография (стеганографические программные продукты) базируется на двух основных принципах:

- D файлы, содержащие оцифрованное изображение или звук, могут быть до некоторой степени видоизменены без потери своей функциональности, в отличие от других типов данных, требующих абсолютной точности;
- ❑ органы чувств человека неспособны различить незначительные изменения в цвете изображения или в качестве звука.

Например, мы отправляем нашему корреспонденту по электронной почте файл с растровой черно-белой картинкой, в котором наименее значащий бит в коде яркости каждой точки изображения будет элементом нашего тайного сообщения. Получатель письма извлечет все такие биты и составит из них «истинное» сообщение. Картинка, присутствующая здесь только для отвода глаз, так и останется для непосвященных простой картинкой.

По аналогии с криптографической системой введем понятие стеганографической системы или, как ее еще называют более сокращенно, стегосистемы.

Стеганографическая система, или стегосистема, — это совокупность средств и методов, которые используются для формирования скрытого канала передачи информации. Модель обобщенной стегосистемы представлена на рис. 5.1.

При построении любой стегосистемы должны учитываться следующие положения:

- ❑ противник имеет полное представление о стеганографической системе, деталях ее реализации, и единственной информацией, которая остается неизвестной потенциальному противнику, является ключ, с помощью которого только его держатель может установить факт присутствия и содержание скрытого сообщения;
- О если противник каким-то образом узнает о факте существования скрытого сообщения, это не должно позволить ему извлечь подобные сообщения в других данных до тех пор, пока ключ хранится в тайне;
- ❑ потенциальный противник должен быть лишен каких-либо технических и иных преимуществ в распознавании или раскрытии содержания тайных сообщений.

В стегосистеме в качестве данных может использоваться любая информация: текст, сообщение, изображение и т. п. В общем же случае, для обозначения скрываемой информации, целесообразно использовать слово «сообщение», так как сообщением может быть как текст или изображение, так и, например, аудиоданные. В современной компьютерной стеганографии существует два основных типа файлов: сообщение — файл, который предназначен для скрытия, и контейнер — файл, который может быть использован для скрытия в нем сообщения.

Сообщение, которое необходимо передать отправителю, с помощью специального программного обеспечения встраивается в контейнер. Контейнер — любая информация, предназначенная для сокрытия тайных сообщений. Данные контейнера должны быть достаточно шумными, чтобы небольшое изменение в их беспорядочности не могло быть заметным. Биты контейнера, хотя и являются шумом сточки зрения точности измерений, могут иметь некоторые специальные статистические характеристики. Предполагается, что кодирование тайного сообщения должно воспроизводить характеристики шума контейнера. Цель труднодостижимая, но реальная. Поэтому выбор контейнера оказывает существенное влияние на надежность всей стегосистемы и возможность

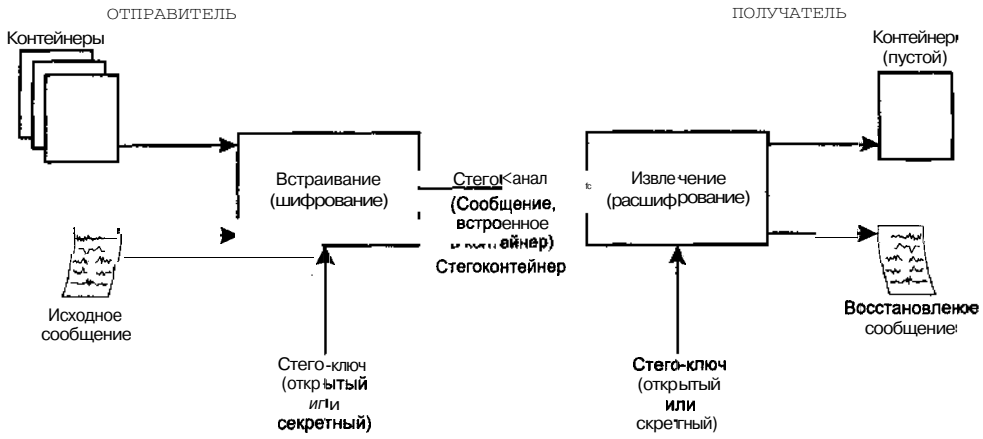


Рис. 5.1. Обобщенная стегосистема

обнаружения факта передачи скрытого сообщения. Например, опытный глаз цензора с художественным образованием легко обнаружит изменение цветовой гаммы при внедрении сообщения в репродукцию «Мадонны» Рафаэля или «Черного квадрата» Малевича.

Возможны следующие варианты контейнеров:

- контейнер генерируется самой стегосистемой;
- контейнер выбирается из некоторого множества контейнеров;
- контейнер поступает извне;
- контейнер, получаемый с помощью моделирования шумовых характеристик.

Примером генерации контейнера самой стегосистемой может служить программа MandelSteg, в которой в качестве контейнера для встраивания сообщения генерируется фрактал Мандельброта. Такой подход получения стегосообщения можно назвать конструирующей стеганографией.

Если используется выборка контейнера из некоторого множества, то в этом случае первоначально генерируется большое число альтернативных контейнеров, чтобы затем выбрать наиболее подходящий для сокрытия сообщения. Такой подход к выбору контейнера называют селектирующей стеганографией. В данном случае при выборе оптимального контейнера из множества сгенерированных важнейшим требованием является естественность контейнера. Единственной же проблемой остается то, что даже оптимально организованный контейнер позволяет спрятать незначительное количество данных при очень большом объеме самого контейнера.

В случае, когда контейнер поступает извне, отсутствует возможность выбора контейнера и для сокрытия сообщения берется первый попавшийся контейнер, не всегда подходящий к встраиваемому сообщению. Такой подход называется безальтернативной стеганографией.

Следующий шаг — моделирование характеристик шума контейнера. Подражательная функция должна быть построена так, чтобы не только кодировать секретное сообщение, но и придерживаться модели первоначального шума. В предельном случае це-

лое сообщение конструируется в соответствии с моделью шума. Такой подход называют конструирующей стеганографией, и он также имеет много недостатков. Его трудно совместить с сильным алгоритмом шифрования, да и моделирование шума или компонентов ошибок в данных — занятие не из легких. Формирование модели требует значительных усилий, творческой работы над каждым каналом связи или контейнером.

Поскольку попытки подражания первоначальному шуму либо ведут к сомнительной безопасности или к слишком малому диапазону рабочих частот для большинства практических применений, наиболее привлекательной остается следующая базовая процедура.

Выбирается класс достаточно шумных контейнеров и идентифицируются биты шума. Затем определяется, какую порцию шумовых битов контейнера можно заменить псевдослучайными данными без значительного изменения его статистических характеристик. Так, если контейнер представляет собой цифровую фотографию, нас должны интересовать младшие биты градаций серой шкалы или RGB-значений при цветном изображении, либо коэффициенты Фурье в JPEG-формате изображений. Изменяя в среднем, допустим, только 100-й пиксель изображения, в одном мегабайте несжатого изображения можно спрятать примерно один килобайт тайных данных.

Для дополнительной безопасности и придания тайному сообщению вида случайных данных оно должно быть зашифровано сильным криптоалгоритмом. Замена псевдослучайными битами некоторых наиболее шумных битов контейнера только немного увеличит уровень шума сообщения, Включение открытого текста в контейнер может заметно изменить его статистические характеристики. Более того, последовательность скрывающих битов должна выбираться псевдослучайным способом как функция секретного ключа. Иначе противник, имеющий алгоритм, без труда вскроет контейнер.

Но и шифрование с ключом не освобождает от проблем. Если скрывающие биты в подозреваемом сообщении имеют некоторые статистические отклонения от других аналогичных сообщений, то противник получит все основания для вывода, что оно содержит скрытые данные. Тогда путем дополнительного зашумления он может исказить сообщение и этим фактически его уничтожить.

По протяженности контейнеры можно подразделить на два типа:

- непрерывные (потоковые);
- ограниченной (фиксированной) длины.

Они представляют собой или поток непрерывных данных, подобно цифровой телефонной связи, или файл, подобный растровому изображению.

Особенностью потокового контейнера является то, что невозможно определить его начало или конец. Более того, нет возможности узнать заранее, какими будут последующие шумовые биты, что приводит к необходимости включать скрывающие сообщение биты в поток в реальном масштабе времени, а сами скрывающие биты выбираются с помощью специального генератора, задающего расстояние между последовательными битами в потоке. Такой способ называют произвольно-интервальным методом. Следует заметить, что в достаточно длинном контейнере можно скрывать несколько сообщений.

В непрерывном потоке данных самая большая трудность для получателя заключается в определении момента, когда же начинается скрытое сообщение. В простом случае, если поток данных имеет конечную длину и часто вновь открывается, тайное со-

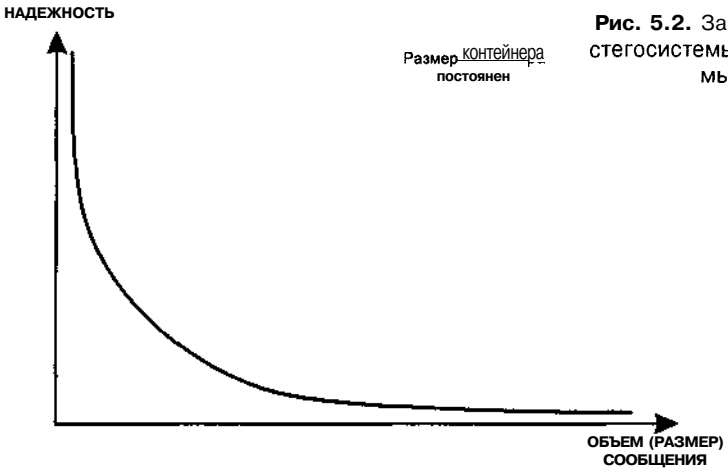


Рис. 5.2. Зависимость надежности стегосистемы от объема встраиваемых сообщении

общение может начинаться при открытии сеанса. При наличии в потоковом контейнере сигналов синхронизации или границ пакета скрытое сообщение начинается сразу же после одного из них. В свою очередь, для отправителя возможны проблемы, если он не уверен в том, что поток контейнера будет достаточно долгим для размещения целого тайного сообщения.

При использовании контейнеров фиксированной длины, которые свободны от недостатков потоковых контейнеров, отправитель заранее знает размер файла и может выбрать скрывающие биты в подходящей псевдослучайной последовательности. Поскольку контейнер известен заранее, есть время оценить его эффективность применительно к выбранному алгоритму сокрытия информации. С другой стороны, контейнеры фиксированной длины имеют ограниченный объем и иногда встраиваемое сообщение может не поместиться в файл-контейнер.

Другой недостаток заключается в том, что расстояния между скрывающими битами равномерно распределены между наиболее коротким и наиболее длинным заданными расстояниями, в то время как истинный случайный шум будет иметь экспоненциальное распределение длин интервала. Конечно, можно породить псевдослучайные экспоненциально распределенные числа, но этот путь обычно слишком трудоемок. Однако на практике чаще всего используются именно контейнеры фиксированной длины, как наиболее распространенные и доступные.

Для большинства современных методов, используемых для сокрытия сообщения в цифровых контейнерах, имеет место зависимость надежности системы от объема встраиваемых сообщений, представленная на рис. 5.2.

Данная зависимость показывает, что при увеличении объема встраиваемых сообщений снижается надежность системы (при неизменности размера контейнера). Таким образом, используемый в стегосистеме контейнер накладывает ограничения на размер встраиваемых данных.

В любом случае контейнер без встроенного сообщения — это пустой контейнер, а контейнер, содержащий встроенную информацию, — это заполненный или стегоконтейнер.

Встроенное (скрытое) сообщение, находящееся в стегоконтейнере, передается от отправителя к получателю по каналу передачи, который называется стеганографическим каналом или просто стегоканалом.

Встраивание сообщений в контейнер происходит с использованием специального стегоключа. Под ключом понимается секретный элемент, который определяет порядок занесения сообщения в контейнер.

По аналогии с криптографией, по типу стегоключа все стегосистемы можно подразделить на два типа:

- с секретным ключом;
- с открытым ключом.

В стегосистеме с секретным ключом используется один ключ, который должен быть определен либо до начала обмена секретными сообщениями, либо передан по защищенному каналу.

В стегосистеме с открытым ключом для встраивания и извлечения сообщения используются разные ключи, которые различаются таким образом, что с помощью вычислений невозможно вывести один ключ из другого. Поэтому один ключ (открытый) может передаваться свободно по незащищенному каналу связи. Кроме того, данная схема хорошо работает и при взаимном недоверии отправителя и получателя.

В зависимости от количества уровней защиты информации (например, встраивание предварительно зашифрованного сообщения) в стегосистеме может быть один или несколько стегоключей.

Любая используемая стегосистема должна отвечать следующим требованиям:

- D свойства контейнера должны быть модифицированы, чтобы изменение невозможно было выявить при визуальном контроле;
- О стегосообщение должно быть устойчиво к искажениям, в том числе и злонамеренным;
- для сохранения целостности встраиваемого сообщения необходимо использование кода с исправлением ошибок;
- О для повышения надежности встраиваемое сообщение должно быть продублировано.

Модификация свойств контейнера определяет качество сокрытия внедряемого сообщения: для обеспечения беспрепятственного прохождения стегосообщения по каналу связи оно никоим образом не должно привлечь внимание атакующего.

В ходе процесса передачи сообщение (звук или другой контейнер) может претерпевать различные трансформации: уменьшаться или увеличиваться, преобразовываться в другой формат и т. д. Кроме того, оно может быть сжато, в том числе и с использованием алгоритмов сжатия с потерей данных. Именно поэтому стегосообщение должно быть устойчивым к такого рода искажениям.

Для повышения целостности и надежности передачи стегосообщения рекомедуется использовать коды, обнаруживающие и исправляющие ошибки, и передавать сообщение неоднократно, изменяя пути следования.

В настоящее время можно выделить (рис. 5.3) три, тесно связанных между собой и имеющих одни корни, направления приложения стеганографии:

- сокрытие данных (сообщений);
- О цифровые водяные знаки;
- заголовки.

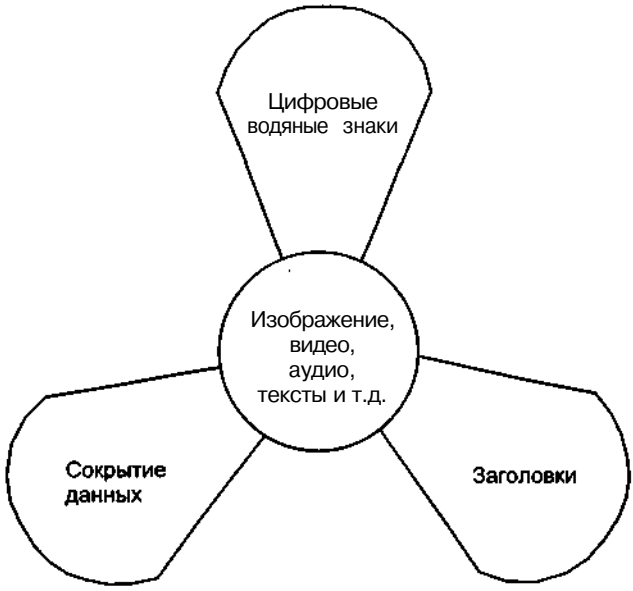


Рис. 5.3. Направления использования компьютерной стеганографии

Сокрытие внедряемых данных, которые в большинстве случаев имеют большой объем, предъявляет серьезные требования к контейнеру. Размер контейнера в несколько раз должен превышать размер встраиваемых данных.

Цифровые водяные знаки используются для защиты авторских или имущественных прав на цифровые изображения, фотографии или другие оцифрованные произведения искусства. Основными требованиями, которые предъявляются к таким встроенным данным, являются надежность и устойчивость к искажениям.

Цифровые водяные знаки имеют небольшой объем, однако, с учетом указанных выше требований, для их встраивания используются более сложные методы, чем для встраивания просто сообщений или заголовков.

Заголовки используются, в основном, для маркирования изображений в больших электронных хранилищах (библиотеках) цифровых изображений, аудио- и видеофайлов. В данном случае стеганографические методы используются не только для внедрения идентифицирующего заголовка, но и иных индивидуальных признаков файла.

Внедряемые заголовки имеют небольшой объем, а предъявляемые к ним требования минимальны: заголовки должны вносить незначительные искажения и быть устойчивы к основным геометрическим преобразованиям.

Каждое из перечисленных выше приложений требует определенного соотношения между устойчивостью встроенного сообщения к внешним воздействиям (в том числе и стегоанализу) и размером самого встраиваемого сообщения.

Далее мы рассмотрим принципы и методы компьютерной стеганографии. Как и любой инструментарий, стеганографические методы требуют к себе серьезного внимания и осторожного обращения: они могут быть использованы как для целей защиты, так и для целей нападения.

Анализ путей практической реализации компьютерной стеганографии

Напомним, что стеганография является наукой, обеспечивающей обмен информацией таким образом, что скрывается сам факт существования секретной связи. Она не заменяет криптографию (шифрование данных), а дополняет ее еще одним уровнем безопасности. Как мы уже говорили, при обработке данных стеганографическими методами происходит скрытие передаваемой информации в других объектах (файлах, дисках и т. п.) таким образом, чтобы постороннее лицо не могло догадаться о существовании скрытого секретного сообщения. При этом обнаружить такое сообщение довольно сложно, но если это и произойдет, то сообщение может быть к тому же еще и надежно зашифровано. При реализации методов стеганографии на компьютере (компьютерная стеганография) определяющим фактором является выбор способа кодирования данных.

Современный прогресс в области глобальных компьютерных сетей и средств мультимедиа привел к разработке новых методов, предназначенных для обеспечения безопасности передачи данных по каналам телекоммуникаций. Эти методы, учитывая естественные неточности устройств оцифровки и избыточность аналогового видео или аудиосигнала, позволяют скрывать сообщения в компьютерных файлах (контейнерах). Причем, в отличие от криптографии, данные методы скрывают сам факт передачи информации. Компьютерные технологии придали новый импульс развитию и совершенствованию стеганографии, и на свет появилось новое направление в области защиты информации — компьютерная стеганография.

Анализ тенденций развития компьютерной стеганографии показывает, что в ближайшие годы интерес к развитию ее методов будет усиливаться все больше и больше. Предпосылки к этому уже сформировались сегодня. В частности, общеизвестно, что актуальность проблемы информационной безопасности постоянно растет и стимулирует поиск новых методов защиты информации. С другой стороны, бурное развитие информационных технологий обеспечивает возможность реализации этих новых методов защиты информации. И, конечно, сильным катализатором этого процесса является развитие глобальной компьютерной сети общего пользования Internet, а также такие нерешенные противоречивые проблемы Internet, как защита авторского права, защита прав на личную тайну, организация электронной торговли, противоправная деятельность хакеров, террористов и т.п.

В настоящее время весьма характерной тенденцией в области защиты информации является внедрение криптологических методов. Однако на этом пути много еще нерешенных проблем, связанных с разрушительным воздействием на криптосредства таких составляющих информационного оружия, как компьютерные вирусы, логические бомбы, различного вида криптоатаки и т. п. Объединение методов компьютерной стеганографии и криптографии является хорошим выходом из создавшегося положения. В этом случае

возможно устранить слабые стороны известных методов защиты информации и разработать новые более эффективные нетрадиционные методы обеспечения информационной безопасности.

Несмотря на то что стеганография как способ сокрытия секретных данных известна уже на протяжении тысячелетий, компьютерная стеганография — молодое и развивающееся направление. Как и любое новое направление, компьютерная стеганография, несмотря на большое количество открытых публикаций и ежегодные конференции, долгое время не имела единой терминологии.

До недавнего времени для описания модели стеганографической системы использовалась предложенная 1983 году Симмонсом так называемая «проблема заключенных». Она состоит в том, что два индивидуума хотят обмениваться секретными сообщениями без вмешательства охранника, контролирующего коммуникационный канал. При этом имеется ряд допущений, которые делают эту проблему более или менее решаемой. Первое допущение облегчает решение проблемы и состоит в том, что участники информационного обмена могут разделять секретное сообщение (например, используя кодовую клавишу) перед заключением. Другое допущение, наоборот, затрудняет решение проблемы, так как охранник имеет право не только читать сообщения, но и модифицировать (изменять) их. Позднее, на конференции Information Hiding: First Information Workshop в 1996 году было предложено использовать новую единую терминологию и обговорены основные термины.

В настоящее время все более актуальной становится проблема обеспечения безопасности связи, под которой можно понимать использование специальных средств, методов и мероприятий с целью предотвращения потери, хищения, копирования и искажения передаваемой конфиденциальной информации. Причем, меры безопасности могут быть направлены как на предотвращение несанкционированного съема защищаемой информации, так и на сокрытие самого факта ее передачи путем использования стандартных технических средств, обычных протоколов информационного обмена и общедоступных каналов связи.

Особую популярность в последнее время получила часть стеганографии, которая использует для сокрытия конфиденциальных сообщений графические изображения, передаваемые по вычислительным сетям. Однако по целому ряду причин, в первую очередь из-за уже достаточной распространенности, невысокой оперативности и информационной эффективности, некоторой сложности процессов обработки, синхронизации и закладки-выкладки полезной информации в изображения-контейнеры, такой вид сокрытия передаваемых конфиденциальных данных не всегда удобен в практической деятельности служб защиты информации предприятий и учреждений.

В связи с возрастанием роли глобальных компьютерных сетей становится все более важным значение стеганографии. Анализ информационных источников компьютерной сети Internet позволяет сделать вывод, что в настоящее время стеганографические системы активно используются для решения следующих основных задач:

О защита конфиденциальной информации от несанкционированного доступа;

О преодоление систем мониторинга и управления сетевыми ресурсами;

G камуфлирования программного обеспечения;

О защита авторского права на некоторые виды интеллектуальной собственности.

Остановимся подробнее на каждой из перечисленных задач.

Защита конфиденциальной информации от несанкционированного доступа с использованием компьютерной стеганографии является наиболее эффективным применением при решении проблемы защиты конфиденциальной информации. Так, например, только одна секунда оцифрованного звука с частотой дискретизации 44100 Гц и уровнем отсчета 8 бит в стереорежиме позволяет скрыть за счет замены наименее значимых младших разрядов на скрываемое сообщение около 10 Кбайт информации. При этом изменение значений отсчетов составляет менее 1% и оно практически не обнаруживается при прослушивании измененного файла большинством людей.

Стеганографические методы, направленные на противодействие системам мониторинга и управления сетевыми ресурсами промышленного шпионажа, позволяют противостоять попыткам контроля над информационным пространством при прохождении информации через серверы управления локальных и глобальных вычислительных сетей.

Другой важной задачей стеганографии является камуфлирование программного обеспечения. В тех случаях, когда использование программного обеспечения незарегистрированными пользователями является нежелательным, оно может быть закамуфлировано под стандартные универсальные программные продукты (например, текстовые редакторы) или скрыто в файлах мультимедиа (например, в звуковом сопровождении компьютерных игр).

При защите авторских прав с использованием стеганографии одним из наиболее перспективных направлений ее развития являются цифровые водяные знаки (digital watermarking). Создание невидимых глазу водяных знаков используется для защиты авторских прав на графические и аудиофайлы. Такие цифровые водяные знаки, помещенные в файл, могут быть распознаны только специальными программами, которые извлекут из файла много полезной информации: когда создан файл, кто владеет авторскими правами, как вступить в контакт с автором. При том повальном воровстве, которое происходит в Internet, польза этой технологии очевидна.

Основными положениями современной компьютерной стеганографии являются следующие:

- методы скрытия должны обеспечивать аутентичность и целостность файла;
- предполагается, что противнику полностью известны возможные стеганографические методы;
- безопасность методов основывается на сохранении стеганографическим преобразованием основных свойств открыто передаваемого файла при внесении в него секретного сообщения и некоторой неизвестной противнику информации — ключа;
- даже если факт скрытия сообщения стал известен противнику через сообщника, извлечение самого секретного сообщения представляет сложную вычислительную задачу.

Методы компьютерной стеганографии

В настоящее время существует достаточно много различных компьютерных методов (и их вариантов) встраивания сообщений. Сегодня методы компьютерной стеганографии (рис. 5.4) развиваются по двум основным направлениям:

- методы, основанные на использовании специальных свойств компьютерных форматов;
- методы, основанные на избыточности аудио- и визуальной информации.

Таблица 5.1. Сравнительные характеристики компьютерных стеганографических методов

Компьютерные стеганографические методы				
Методы использования специальных свойств компьютерных форматов данных				
Наименование	Методы использования зарезервированных для расширения полей компьютерных форматов данных	Методы специального форматирования текстовых файлов:		
		Методы использования известного смещения слов, предложений, абзацев	Методы выбора определенных позиций букв (нулевой шифр)	Методы использования специальных свойств полей форматов, не отображаемых на экране
Краткая характеристика	Поля расширения имеются во многих мультимедийных форматах, они заполняются нулевой информацией и не учитываются программой	Методы основаны на изменении положения строк и расстановки слов в предложении, что обеспечивается вставкой дополнительных пробелов между словами	Акростих — частный случай этого метода (например, начальные буквы каждой строки образуют сообщение)	Методы основаны на использовании специальных «невидимых», скрытых полей для организации сносок и ссылок (например, использование черного шрифта на черном фоне)
Недостатки	Низкая степень скрытности, передача небольших ограниченных объемов информации	Слабая производительность метода, передача небольших объемов информации. Низкая степень скрытности		
Преимущества	Простота использования	Простота использования. Имеется опубликованное программное обеспечение реализации данного метода		

Сравнительные характеристики существующих стеганографических методов приведены в табл. 5.1. Как видно из этой таблицы, первое направление основано на использовании специальных свойств компьютерных форматов представления данных, а не на избыточности самих данных. Специальные свойства форматов выбираются с учетом защиты скрываемого сообщения от непосредственного прослушивания, просмотра или прочтения.

Продолжение табл. S, 1

			Методы использования избыточности аудио— и визуальной информации	
Методы скрытия в неиспользуемых местах гибких дисков	Методы использования имитирующих функций (mimic–function)	Методы удаления идентифицирующего файл заголовка	Методы использования избыточности цифровой фотографии ицифрового видео	Методы использования избыточности цифрового звука
Информация записывается в обычно неиспользуемых местах ГМД (например, в нулевой дорожке)	Метод основан на генерации текстов и является обобщением акростиха. Для тайного сообщения генерируется осмысленный текст, скрывающий само сообщение	Скрываемое сообщение шифруется и у результата удаляется идентифицирующий заголовок, оставляя только шифрованные данные. Получатель заранее знает о передаче сообщения и имеет недостающий заголовок	Младшие разряды цифровых отсчетов содержат очень мало полезной информации. Их заполнение дополнительной информацией практически не влияет на качество восприятия, что и дает возможность скрытия конфиденциальной информации	
Слабая произвольность метода, передача небольших объемов информации. Низкая степень скрытности	Слабая произвольность метода, передача небольших объемов информации. Низкая степень скрытности	Проблема скрытия решается только частично. Необходимо заранее передать часть информации получателю	За счет введения дополнительной информации искажаются статистические характеристики цифровых потоков. Для снижения компрометирующих признаков требуется коррекция статистических характеристик	
Простота использования. Имеется опубликованное программное обеспечение реализации данного метода	Результирующий текст не является подозрительным для систем мониторинга сети	Простота реализации. Многие средства (White Noise Storm, S–Tools), обеспечивают реализацию этого метода с PGP шифроалгоритмом	Возможность скрытой передачи большого объема информации. Возможность защиты авторского права, скрытого изображения товарной марки, регистрационных номеров и т. п.	

Второе направление использования стеганографии в компьютерных системах основано на использовании избыточности аудио и визуальной информации. Цифровые фотографии, цифровая музыка, цифровое видео — представляются матрицами чисел, которые кодируют интенсивность сигналов в дискретные моменты в пространстве и/или во времени. Цифровая фотография — это матрица чисел, представляющих интенсивность света в определенный момент времени. Цифровой звук — это матрица чи-

Рис. 5.4. Компьютерные стеганографические методы

сел, представляющая интенсивность звукового сигнала в последовательно идущие моменты времени.

Все эти числа не точны, т. к. не точны устройства оцифровки аналоговых сигналов. Погрешность измерений последних зависит от суммы погрешностей блока преобразований и датчика, преобразующего физическую характеристику сигнала в электрический сигнал. Эти погрешности измерений обычно выражаются в процентах или в количестве младших значащих разрядов и называются шумами квантования. Младшие разряды цифровых отсчетов содержат очень мало полезной информации о текущих параметрах звука и визуального образа, что позволяет использовать их для сокрытия дополнительной информации.

Например, графические цветные файлы со схемой смешения RGB кодируют каждую точку рисунка тремя байтами (по одному для каждого из цветов). Поэтому каж-

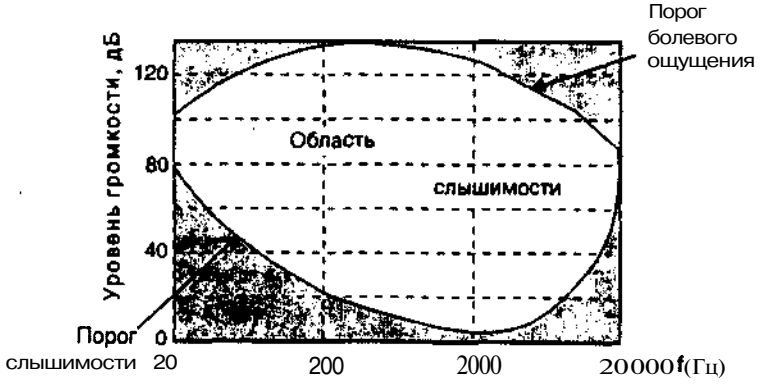


Рис. 5.5. Окно слышимости человека

дая такая точка состоит из составляющих: красного, зеленого, синего цветов соответственно. Изменение каждого из трех наименее значимых бит приводит к изменению шится. Если изменения происходят не в каждом отсчете, то объем передаваемых данных уменьшается, но снижается вероятность их обнаружения.

При использовании компьютерной стеганографии придерживаются следующих принципов:

- в качестве носителя скрытой информации должен выступать объект (файл), допускающий искажения собственной информации, не нарушающие его функциональность и суть;
- внесенные искажения должны быть ниже уровня чувствительности средств распознавания.

Первый заключается в том, что файлы, содержащие оцифрованное изображение или звук, могут быть до некоторой степени видоизменены без потери функциональности, в отличие от других типов данных, требующих абсолютной точности.

Второй фактор состоит в неспособности органов чувств человека различить незначительные изменения в цвете изображения или качестве звука, что особенно легко использовать применительно к объекту, несущему избыточную информацию, будь то 16-битный звук, 8-битное или еще лучше 24-битное изображение. Если речь идет об изображении, то изменение значений наименее важных битов, отвечающих за цвет пиксела, не приводит к заметному для человеческого глаза изменению цвета.

Если речь идет о звуке, то, как видно из рис. 5.5, в этом случае учитывается так называемое окно слышимости человека. Из рисунка видно, что не все звуковые частоты органы слуха человека воспринимают одинаково. Верхняя граница окна соответствует оглушительному звуку, соседствующему с болевым ощущением. Нижняя граница определяется порогом слышимости. Кроме того, человек практически не может однозначно регистрировать на слух изменения интесивности звука, если она изменяется очень и очень незначительно.

Стеганографические алгоритмы обработки звука строятся с таким расчетом, чтобы максимально использовать окно слышимости и другие свойства речевых сигналов (тембр, скорость и т.д.), незначительные изменения которых не слышны человеку.

Особенности скрытой передачи аудиоинформации

Особенности психоакустики восприятия человеком звуковых колебаний позволяют скрытно передавать информацию через речевое сообщение. Среди всех известных психоакустических эффектов наиболее предпочтительным для решения этой задачи является эффект маскировки. Суть этого эффекта сводится к следующему. Более интенсивные речевые отрезки делают неслышимыми сигналы, появившиеся до них («маскировка вперед») и после них («маскировка назад»). Временной диапазон маскировки вперед простирается до 20 мс, а назад — до 150 мс. Кроме того, существует и частотная маскировка, когда в момент появления более интенсивного низко-частотного сигнала становится неслышным более высокочастотный сигнал меньшей амплитуды. Необходимо отметить, что подъем высоких частот уменьшает диапазон частотной маскировки.

Маскировка вперед в речевом сигнале наиболее отчетливо проявляется на открытых взрывных слогах, средняя вероятность появления которых в русской речи состав-

ляет 0,18. Средняя длительность открытого взрывного слога составляет около 120 мс, что означает, что на одну секунду речи дополнительное кодирование с помощью маскировки назад в среднем может занять временной интервал длительностью всего 3,6 мс. Количество квантов скрытой информации на одну секунду речи равняется 0,9, т. е. за 1,1 секунду речи можно передать один квант длительностью 3,6 мс. Квант скрытой информации может быть синусоидальным сигналом длительностью 3,6 мс. Под квантом понимается некоторый блок, элемент данных, характеризующийся некоторым набором логических параметров — атрибутов, таких как формат, длина, частота, амплитуда, фаза и т.д.

Маскировка назад в речевом сигнале может возникать в двух случаях.

Во-первых, в моменты прекращения фонации, т.е. выключения тонального источника. Здесь следует учесть особенности работы тонального источника в этот момент. Колебания голосовых связок происходят с уменьшением амплитуды и сужением спектра генерируемых колебаний вплоть до частоты основного тона. Таким образом, в этот момент в речевом сигнале отсутствуют высокочастотные колебания. Квант скрытой информации может представлять собой широкополосный шумоподобный сигнал с убывающей по частоте спектральной энергетикой и с убывающей интенсивностью во времени. Известно, что вероятность появления гласных звуков в русской речи составляет 0,3, а с выключением фонации она уменьшается приблизительно в 3—4 раза. Средняя длительность прекращения фонации около 70 мс. Таким образом, на одну секунду речи можно передать до 7 мс скрытой информации. Этот механизм кодирования включает как маскировку назад, так и частотную маскировку. Поскольку фаза выключения тонального источника находится во временной зоне маскировки назад, то появляется возможность регулировать спад интенсивности, например по экспоненциальному или временному закону. Это дает еще дополнительных 7 мс для передачи скрытой информации и увеличивает количество квантов скрытой информации до 2 на одну секунду речи.

Во-вторых, при переходе от гласных звуков с низкой первой резонансной частотой [у, и, ы] к сонорным [л, м, н] происходит уменьшение амплитуды в два раза. Вероятность такого эффекта составляет 0,3, а вероятность появления таких слогов 0,024. Длительность маскировки назад в таком случае уменьшается до 30—50 мс, так что за одну секунду речи можно передать 0,5 мс скрытой информации. Количество квантов скрытой информации на одну секунду речи 0,1.

Перейдем к частотной маскировке. Этот механизм может работать практически всегда, когда работает тональный источник возбуждения речевого тракта. Кванты кодируемого сообщения могут представлять собой дополнительные более высокочастотные и менее интенсивные суммы синусоид, чем основные компоненты тонального речевого сигнала. Вероятность появления тональных отрезков в русской речи равна 0,7, следовательно, длительность кодируемого участка может равняться 500—600 мс на одну секунду речи, а количество квантов скрытой информации при средней длительности кванта 50 мс достигать 10—12.

Рассмотрим ограничения, связанные с ограниченными возможностями нашей слуховой системы, которые позволяют внедрять дополнительную скрытую информацию.

Первое ограничение связано с нечувствительностью нашей слуховой системы к провалам спектра в шумовом сигнале. Таким образом, используя режекторную филь-

трацию, можно на звуках речевого сообщения, порожденных турбулентным источником, передавать дополнительную информацию. Эти частоты для звука [х] расположены в диапазоне частот ниже 800 Гц, для звука [ш] в диапазоне частот от 2 кГц до 4 кГц, а для звука [с] на частотах выше 5 кГц. Вероятность встретить перечисленные звуки в русской речи равна 0,08, так, что за одну секунду речи можно передать 80 мс скрытой информации и количество квантов скрытой информации составит 1,2 на одну секунду речи.

Второе ограничение связано с чувствительностью нашей слуховой системы к изменению значений ширин резонансов, возникающих в речевом тракте. Такая относительная чувствительность составляет 30%. Это означает, что речевой сигнал можно корректировать, изменяя добротности резонансов гласных звуков. В этом случае есть возможность внедрить до 200—300 мс скрытой информации на одну секунду речи с количеством квантов скрытой информации 2—3 за одну секунду речи.

Третье ограничение связано с возможностью регулирования речевого сигнала на интервалах вынужденных (моменты времени, когда ускорения воздушного потока, порожденные работой голосовых связок, максимальны) и свободных (когда влияние голосовых связок отсутствует) колебаний. Регулировать длительность этих интервалов нельзя, поскольку наше слуховое восприятие очень чувствительно к этим изменениям. Однако увеличить амплитуду на интервалах вынужденных колебаний можно. Но делать это надо очень аккуратно, корректируя диапазон изменения мгновенной частоты для каждого резонанса речевого тракта. Интервал вынужденных колебаний не превосходит половины периода низкочастотного резонанса в речевом тракте, т. е. частоту 300—600 Гц. С учетом частоты основного тона 100—200 Гц и длительности гласных звуков русской речи 200—300 мс на одну секунду речи (с учетом релаксационного режима колебаний голосовых связок с широким спектром гармоник), получаем общую длительность кодирования до 45 мс. Следует отметить, что этот вид кодирования является наиболее сложным для обнаружения с помощью современных методов анализа и распознавания речевых сигналов. Количество квантов скрытой информации при этом составит от 15 до 40 на одну секунду речи.

Перейдем к возможности внедрения специфических, не мешающих восприятию речевого сигнала, помех. В качестве таких сигналов могут рассматриваться возбуждения на дополнительных резонансных частотах. Возбуждения осуществляются импульсами тонального источника, выделенными из самого же исходного речевого сигнала. Этот механизм можно рекомендовать для тех интервалов, на которых порождаются гласные звуки. Новые резонансы не мешают пониманию исходного речевого сигнала и на слух воспринимаются как некоторое улучшение тембральности исходного речевого сообщения. Длительность таких аддитивных сигналов составляет 500—600 мс, а количество передаваемых квантов скрытого сообщения от 2 до 4 на одну секунду речи.

Таким образом, максимальная скорость передачи скрытой информации на речевом сигнале может быть 52,2 кванта за одну секунду. Самый простой способ кодирования — это режекция звуков, порожденных турбулентным источником, со скоростью передачи 1 квант в секунду. Самым трудным для обнаружения эффекта кодирования является метод коррекции речевого сигнала на временных участках вынужденных колебаний с минимальной скоростью передачи информации 12 квантов. Информационная емкость каждого кванта в среднем может составить 2 бита (примерно 4 состояния),

так что максимальная скорость передачи информации может составить примерно 100 бит в секунду. Любопытно отметить, что и скорость передачи вербального компонента речевого сигнала составляет 50—100 бит в секунду.

Теоретически диапазон возможных методов стеганографии соизмерим с широтой человеческого воображения. Поэтому ограничимся лишь теми подходами к проблеме, которые уже получили распространение. На практике стеганографические системы, построенные по второму принципу, используются наиболее часто, несмотря на многие, присущие этому методу, недостатки. Наиболее простым и популярным в компьютерной стеганографии является так называемый метод, основанный на использовании младшего бита звуковых (и/или любых других мультимедийных) данных — LBS-метод (Least Significant Bits). Рассмотрим этот метод более подробно на примере использования звуковых сигналов.

Начнем с того, что львиная доля компьютерной информации «шумит». «Шумит» все то, что хранится, передается и обрабатывается. Далее кавычки убираем, так как это законный технический термин, указывающий на наличие ошибок в данных, помех в каналах связи и прочих случайных сигналов и знаков. Так как речевой сигнал записывается с микрофона, то в записи присутствует некоторый уровень шума, зависящий от качества микрофона, уровня внешних акустических помех и погрешностей устройств преобразования аналогового сигнала в цифровой.

Естественные шумы, которые содержат цифровые массивы аудиоданных, полученные стандартными способами преобразования из аналоговых акустических сигналов, являются ошибками квантования и не могут быть полностью устранены. Использование шумовых бит для передачи дополнительной конфиденциальной информации позволяет создавать скрытый канал передачи данных. В этом смысле здесь прослеживается некоторая аналогия с традиционными методами скрытия данных в изображениях. В качестве шумовых бит обычно рассматриваются младшие разряды значений отсчетов, которые являются шумом с точки зрения точности измерений и несут наименьшее количество информации, содержащейся в отсчете. Рассмотрим, как эти преобразования происходят.

Минимальной единицей хранения информации в компьютере, как известно, является бит. Любое значение — это совокупность битов. Именно из этих битов состоит «оцифрованный» аналоговый сигнал после преобразования с помощью аналогоцифрового преобразователя (АЦП). При использовании компьютера эти преобразования выполняются звуковой картой, разрядность которой существенно влияет на качество звука. В недавнем прошлом прямое указание на разрядность звуковой карты содержалось в ее названии в виде числа 16. Тем самым изготовители подчеркивали, что в их продукции качество цифрового звука как бы соответствует качеству звука лазерного проигрывателя, а не какой-нибудь там 8-битной карты. В дальнейшем 16 разрядов в АЦП стали нормой, а числа «32» или «64» в названиях стали означать совсем другое — максимальное количество одновременно звучащих голосов синтезатора звуковой карты (полифонию).

Некоторые высококачественные звуковые карты оборудованы 18-битными и даже 20-битными АЦП. Звуковые редакторы, работая с любыми звуковыми картами, в том числе и 16-битными, в процессе преобразований отсчетов сигнала используют арифметику с разрядностью двоичного представления числа, превышающей 16. Это позво-

ляет уменьшить погрешность, накапливающуюся в процессе выполнения сложных алгоритмов обработки, которая в противном случае проявлялась бы как искажение звука.

Почему же столь важно наличие большого числа разрядов в устройствах АЦП? Дело заключается в том, что непрерывный (аналоговый) сигнал преобразуется в цифровой с некоторой погрешностью. Эта погрешность тем больше, чем меньше уровней квантования сигнала, т. е. чем дальше отстоят друг от друга допустимые значения квантованного сигнала. Число уровней квантования, в свою очередь, зависит от разрядности АЦП. Погрешности, возникающие в результате замены аналогового сигнала рядом квантованных по уровню отсчетов, можно рассматривать как его искажения, вызванные воздействием помехи. Эту помеху принято образно называть шумом квантования. Шум квантования (рис. 5.6) представляет собой разность соответствующих значений реального и квантованного по уровню сигналов.

Из рис. 5.6 видно, что в случае превышения сигналом значения самого верхнего уровня квантования («старшего» кванта), а также в случае, когда значение сигнала оказывается меньше нижнего уровня квантования («младшего» кванта), т. е. при ограничении сигнала, возникают искажения, более заметные по сравнению с шумом квантования. Для исключения искажений этого типа динамические диапазоны сигнала и АЦП должны соответствовать друг другу, иными словами, значения сигнала должны располагаться между уровнями, соответствующими младшему и старшему квантам.

Для нормированного сигнала относительная величина максимальной погрешности квантования равна 1/N, §Ф§Х§Ц N¡ª§й§Ъ§г§Э§а §е§в§а§У§Я§Ц§Ы §Ь§У§С§Я§д-§а§У§С§Я§Ъ§с. §¸§д§а§Ы §Ш§Ц §У§Ц§Э§Ъ§й§Ъ§Я§а§Ы, §б§в§Ц§Х§г§д§С§У§Э§-Ц§Я§Я§а§Ы §У §Э§а§Ф§С§в§Ъ§ж§Ю§Ъ§й§Ц§г§Ь§Ъ§з §Ц§Х§Ъ§Я§Ъ§и§С§з (§Х§Ц§и§Ъ§Т§Ц§Э§С§з), §а§и§Ц§Я§Ъ§У§С§Ц§д§г§с §е§lg(1/N). Для трехразрядного АЦП (см. рис. 5.6) N=8, ? = — 18 дБ; для восьмиразрядного — N=256, ? = — 48дБ; для шестнадцатиразрядного — N=65536, ? = — 96 дБ; для восемнадцатиразрядного АЦП N=262144, ? = — 108 дБ; и для двадцатиразрядного АЦП N= 1648576, ? = — 120 дБ. Эти цифры наглядно демонстрируют, что с ростом разрядности АЦП шум квантования уменьшается. Приемлемым считается 16-разрядное представление сигнала, являющееся в настоящее время стандартным для воспроизведения звука, записанного в цифровой форме. С точки зрения снижения уровня шумов квантования дальнейшее увеличение разрядности АЦП нецелесообразно, т. к. уровень шумов, возникших по другим причинам (тепловые шумы, а также импульсные помехи, генерируемые элементами схем компьютера и распространяющиеся либо по цепям питания, либо в виде электромагнитных волн), все равно оказывается значительно выше, чем — 96 дБ. Но и при использовании 16 разрядного АЦП изменение уровня сигнала, соответствующее младшему значащему разряду или даже двум-трем, практически не воспринимается человеком на слух. Кроме того, при «оцифровке» одного и того же звукового фрагмента с использованием одного и того же АЦП, мы каждый раз будем получать новый «цифровой» фрагмент, отличный от предыдущих хотя бы значением одного младшего разряда.

Однако увеличение разрядности АЦП обусловлено еще одним фактором — стремлением расширить его динамический диапазон. Поэтому динамический диапазон для 16-разрядного АЦП составляет 96 дБ, для 18-разрядного — 108 дБ, для 20-разрядного —

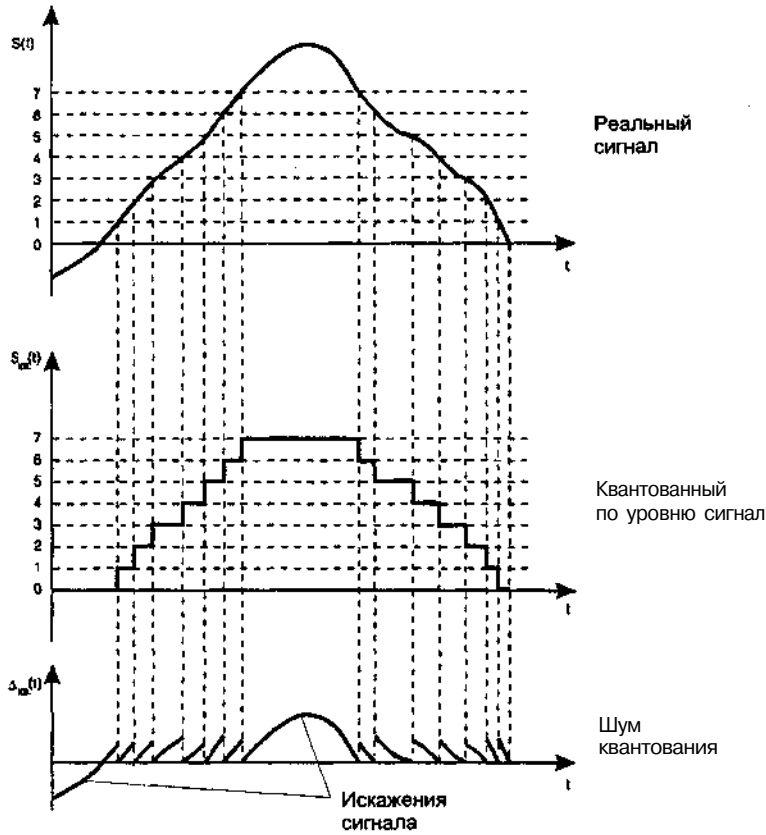


Рис. 5.6. Квантование сигнала по уровню

120дБ. Иными словами, для записи звучания некоторого источника звука, динамический диапазон которого составляет 120 дБ, требуется двадцатиразрядный АЦП. Если такого нет, а имеется только шестнадцатиразрядный, то динамический диапазон звука должен быть сжат на 24 дБ (от 120 дБ до 96 дБ).

После того как мы немного разобрались с разрядностью звуковой карты, пришло время поговорить о частоте дискретизации. В процессе работы АЦП происходит не только квантование сигнала по уровню, но и его дискретизация во времени (рис. 5.7). Сигнал, непрерывно изменяющийся во времени, заменяют рядом отсчетов этого сигнала. Обычно отсчеты сигнала берутся через одинаковые промежутки времени. Интуитивно ясно, что если отсчеты отстоят друг от друга на слишком большие интервалы, то при дискретизации может произойти потеря информации: если важные изменения сигнала произойдут не в те моменты, когда были взяты отсчеты, они могут быть «пропущены» преобразователем. Получается, что отсчеты следует брать с максимальной частотой. Естественным пределом служит быстродействие преобразователя. Кроме того, чем больше отсчетов приходится на единицу времени, тем больший размер памяти необходим для хранения информации.

Проблема отыскания разумного компромисса между частотой взятия отсчетов сигнала и расходованием ресурсов трактов преобразования и передачи информации возникла задолго до того, как на свет появились первые звуковые карты. В результате исследований было сформулировано правило, которое в отечественной научно-технической литературе принято называть теоремой Котельникова. Если поставить перед собой задачу обойтись без формул и использования серьезных научных терминов типа «система ортогональных функций», то суть теоремы Котельникова можно объяснить следующим образом. Сигнал, представленный последовательностью дискретных отсчетов, можно вновь преобразовать в исходный (непрерывный) вид без потери информации только в том случае, если интервал между соседними отсчетами не превышает половины периода самого высокочастотного колебания, содержащегося в спектре сигнала.

Из сказанного следует, что восстановить без искажений можно только сигнал, спектр которого ограничен некоторой максимальной частотой (теоретически все реальные сигналы имеют бесконечные спектры). Для того чтобы при дискретизации избежать искажений, вызванных этим обстоятельством, сигнал вначале пропускают через фильтр, подавляющий в нем все частоты, которые превышают заданное значение максимальной частоты, и лишь затем производят дискретизацию. Если учесть некоторые реальные свойства сигналов, свойств человеческого слуха (окно слышимости) и устройств преобразования, то частоту дискретизации следует выбирать не менее 20 кГц. Так в стандарте CD частота дискретизации равна 44,1 кГц, для цифровых звуковых магнитофонов стандартная частота дискретизации составляет 48 кГц, звуковые карты, как правило, способны работать в широком диапазоне частот дискретизации.

Заменив микрофон на устройство преобразования светового сигнала в электрический можно провести с ним те же преобразования, что и со звуковым сигналом. Поэтому мы лишь кратко поясним суть использования младших разрядов применительно к изображениям.

В 8-битном изображении (RGB кодирование) цвет каждой точки кодируется 8 битами или байтом, например — 00010001. Каждая цветовая комбинация тона (пиксела — точки) — это комбинация трех основных цветов: красного R, зеленого G и синего B, которые занимают каждый по 1 байту (итого по 3 байта на каждую точку). При кодировании стеганографического изображения изменяется последний (младший) бит каждой точки (или, допустим, с определенным шагом) — что приводит к незаметному для большинства людей изменению изображения – цвет части точек, составляющих изображение,

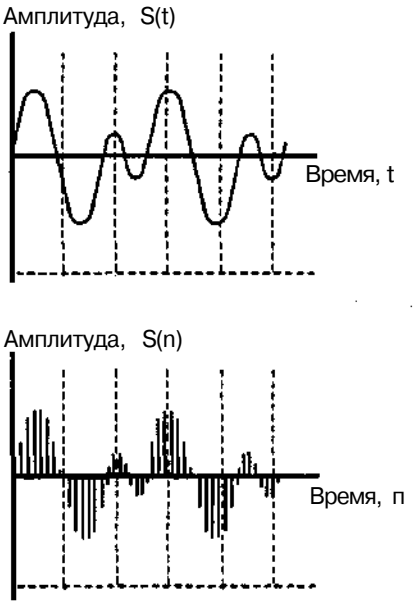


Рис 5.7 Дискретизация сигнала во времени

смещается к соседнему в палитре (более темному или более светлому). Многое зависит, конечно, и от изображения, — чем пестрее оно, чем больше цветов задействовано, тем труднее отличить исходное изображение от изображения, содержащего дополнительную информацию. Если предположить, что в качестве носителя используется 24 битовое изображение размером 800x600 (графика среднего разрешения), то оно будет занимать около полутора мегабайта памяти (800x600x24/8 = 1440000 байт). Если для хранения секретной информации использовать наименьший значащий бит каждого байта, то получим по 3 бита на каждый пиксел. Емкость вносимой в исходное изображение скрываемой информации составит — 800x600x3/8 = 180000 байт. При этом биты последней в некоторых точках будут совпадать с битами реального изображения, в других — нет, но, главное, что на глаз определить такие искажения практически невозможно.

Другим популярным методом встраивания сообщений является использование особенностей форматов данных, использующих сжатие с потерей данных (например, JPEG). Этот метод (в отличие от LSB) более стоек к геометрическим преобразованиям и обнаружению канала передачи, так как имеется возможность в широком диапазоне варьировать качество сжатого изображения, что делает невозможным определение происхождения искажения.

При передаче объемных файлов (например, по — E-mail или через интерактивные службы Internet — WWW и FTP) используются разнообразные методы сжатия, из которых для целей стеганографии предпочтительны те методы, которые обеспечивают сжатие без потерь, поскольку требуется точное восстановление спрятанных данных. Такие виды сжатия типичны для изображений в форматах GIF2, TIFF и BMP, а также звуковых форматов WAV, AU и др.

Среди свойств звуковых данных, оказывающих влияние на обеспечение скрытности конфиденциальной информации и, соответственно, на обеспечение ее безопасности методами с использованием шумовых бит, можно выделить следующие:

- неоднородность последовательностей отсчетов;
- наличие определенных зависимостей между битами в отсчетах;
- наличие определенных зависимостей между самими отсчетами;
- неравновероятность условных распределений в последовательности отсчетов;
- наличие длинных серий одинаковых бит;
- наличие корреляции между НЗБ и старшими битами.

Эти свойства в различной степени наблюдаются в большинстве звуковых файлов и могут быть использованы при построении различных статистических критериев, определяющих факт сокрытия информации в младших значащих разрядах. Вот почему подобные методы компьютерной стеганографии стали применяться на практике все реже.

В то же время, прогресс, достигнутый в области разработки устройств передачи речевых сигналов с использованием средств вычислительной техники, открывает новые возможности для скрытой передачи конфиденциальной информации в аналоговых и цифровых аудиосигналах и речи на основе использования динамично развивающихся технологий мультимедиа, компьютерной и сотовой телефонии.

Сегодня предлагаются следующие требования к сокрытию конфиденциальной информации в аудиосигналах:

О слуховое восприятие речевых и акустических сигналов с заложенной в них скрываемой информацией должно быть практически неотличимым от восприятия исходной, «открытой» речи или звука;

- передаваемые по открытым каналам связи конфиденциальные данные, камуфлированные речевыми или акустическими сигналами или в неявном виде содержащиеся в их параметрах, не должны легко обнаруживаться в этих сигналах-носителях широко распространенными методами и техническими средствами анализа звука и речи, имеющимися в наличии в настоящее время;
- в ряде приложений постановка и выявление стеганофонических маркеров не должны зависеть от синхронизации этих процессов и от наличия каких-либо акустических эталонов;
- специальные методы постановки и выявления стеганофонических маркеров должны реализовываться на основе стандартной вычислительной техники или специальных программно-аппаратных средств на ее основе;
- должна обеспечиваться возможность закладки и обнаружения признаков аутентичности в акустический (речевой) сигнал, проявляющихся при незаконном его копировании или модификации независимо от вида представления и передачи этого сигнала (аналогового или цифрового);
- должна обеспечиваться возможность сокрытия конфиденциальной информации в акустическом (речевом) сигнале независимо от вида его представления (аналогового или цифрового) и передачи в открытых каналах связи.

В большинстве случаев этим требованиям можно удовлетворить, используя новый подход к построению специальных стеганофонических программно-аппаратных средств аудиообработки. Этот подход сочетает идею перевода звукового сигнала в вид графических образов (изображений сонограмм и фазограмм) и обратно без потери информативности и/или разборчивости с возможностями известных и перспективных методов цифровой обработки изображений.

Следы фонообъектов различной природы в виде параметров составляющих их сигналов проявляются на изображениях динамических спектрограмм в виде совокупности контуров (линий) перепада яркости или треков (цепочек) локальных и глобальных экстремумов цветовой насыщенности в уровнях одного цвета. С помощью специального программного обеспечения такие следы, а точнее амплитуды и фазы узкополосных сигналов, контуры или треки которых и видны на частотно-временной сетке динамических спектрограмм, можно реконструировать, модифицировать, уничтожать, создавать заново для решения конкретной стеганофонической задачи.

Так, в ряде программных продуктов, продвигаемых на рынке спецтехники, реализована возможность выборки и обработки узкополосных составляющих интересующего участка изображения спектрограммы исследуемого фонообъекта. К данному участку можно приложить либо собственные, входящие в состав программных продуктов, инструменты цифровой обработки изображений, либо использовать мощный арсенал средств, предоставляемых известными графическими редакторами типа «Adobe Photoshop», после транспортировки и обработки в них выбранного участка спектрограммы с возможностью последующей обратной вставки и синтеза модифицированного таким образом изображения.

Или, аккуратно затирая или подрисовывая с нужным нажимом (амплитудой) отдельные обертона речи на вокализованных участках изображений динамических сонограмм, можно оставлять только их четное или нечетное количество, соответственно, принимая их за значения единичных или нулевых битов конфиденциальной информации в процессе ее передачи-хранения в речевом сигнале. Кроме того, взяв один из обертонов за опорный, можно просинтезировать все остальные обертона с определенным фазовым смещением по отношению к нему. Задавая вектора приведенных начальных фаз, можно достичь достаточно большой емкости внедренных бит сокрываемой информации на единицу времени. Просинтезированная речь будет звучать аналогично исходной, поскольку фазовые отклонения практически не влияют на слуховое восприятие, а огибающие динамических спектров и связанная с ними фонетическая функция не нарушаются. Можно также установить определенную шкалу условных отрезков на временной оси. При целом укладывании в эти отрезки просинтезированных отдельных слов или фраз будем считать, что передан единичный бит информации, а в противном случае — что передан нулевой бит. Также можно ввести шкалу условных отрезков и на частотной оси. Небольшие (до 20%) отклонения темпа и тембра новой речи по отношению к исходной также практически незаметны на слух.

Кроме того, речевой сигнал можно незаметно для слуха передавать и хранить в другой речи, а также сочетать технологии стеганофонии с технологиями стеганографии, «растворяя» изображения динамических акустических спектрограмм в заданных изображениях, с последующим их проявлением и синтезом на приемном конце канала связи. Между тем, и сами изображения сонограмм могут быть использованы для передачи и хранения речи на бумажных носителях. При реализации таких технологий «речевой подписи», связанных с защищаемым документом по смыслу и содержанию примерно так же, как и электронно-цифровая подпись, на стандартный лист бумаги может быть нанесено в виде разнообразных узорчатых рисунков от 2 до 4 минут речи телефонного качества звучания.

На основе предложенной технологии можно осуществить и такой способ простановки стеганофонических маркеров, который заключается в синтезе звукового сигнала по заданному известному изображению для последующего хранения на носителе или передачи в общедоступный канал связи.

С помощью предложенного подхода к обработке звуковых сигналов можно реализовать большое количество самых разнообразных способов компьютерной стеганофонии, эксклюзивных для каждой конкретной задачи.

Следует еще раз отметить, что рассмотренные способы постановки стеганофонических маркеров и внесения информации в исходный речевой сигнал в большинстве случаев не требуют синхронизации процессов их введения. Вследствие этого они могут применяться в каналах связи не только при приеме-передаче, но и в режимах хранения речевых сигналов и звука. Поэтому они могут найти свое применение в аналоговых и цифровых автоответчиках, стандартных системах голосовой почты, компьютерной телефонии и т. п., а также при переносе обработанных речевых сигналов на аудиокассетах и дискетах. Понятно, что совместное применение в предложенных методах компьютерной стеганофонии сертифицированных ФАПСИ алгоритмов криптографического закрытия позволяет повысить стойкость подобных систем к по-

пыткам нарушителя выявить и использовать в своих целях защищаемую конфиденциальную информацию.

Проведенные оценки допустимых значений скорости скрытной передачи конфиденциальной информации в аудиосигналах показали, что на сегодняшний день эти значения не превышают 100 бит/с. Это пока максимальные значения, которые могут быть достигнуты при различных способах сокрытия информации в речевых или акустических сигналах посредством соответствующей обработки графических образов их динамических спектрограмм. Тем не менее, можно предположить, что таких скоростей, скорее всего, будет вполне достаточно для оперативной передачи важных конфиденциальных сообщений в процессе речевого общения двух абонентов по телефонной линии или посредством приема-передачи аудиокассет, содержащих аудиосигналы-контейнеры с информационной закладкой, а также других приложений. Действительно, при таких скоростях в одной минуте речевого сигнала в процессе телефонных переговоров может быть скрытно передано примерно три страницы текста и порядка десяти черно-белых фотоснимков изображения лица.

Способы защиты прав авторской продукции в сети

Кроме скрытой передачи сообщений, стеганография является одной из самых перспективных направлений, применяемых для аутентификации и маркировки авторской продукции. При этом, часто в качестве внедряемой информации используются дата и место создания продукта, данные об авторе, номер лицензии, серийный номер, дата истечения срока работы (удобно для распространения shareware-программ) и др. Эта информация обычно внедряется как в графические и аудиопроизведения, так и в защищаемые программные продукты. Все внесенные сведения могут рассматриваться как веские доказательства при рассмотрении вопросов и судебных разбирательств об авторстве или для доказательства факта нелегального копирования и часто имеют решающее значение.

Компании, торгующие музыкой или видеоизображениями в сети, чтобы хоть как-то приостановить пиратство, пытаются поместить в файлы, ими распространяемые, цифровые водяные знаки, которые, с одной стороны, должны быть как можно менее ощутимы для содержания файла, с другой — должны однозначно идентифицировать владельца копирайта, а с третьей — оставаться незаметными для хакеров, которые попытаются их удалить. Фотоагентства используют их для «мечения» своих изображений. Налоговая служба США не раз предупреждала о том, что некоторые веб-сайты используют этот метод для маскировки картинок с порнографией.

В современных системах формирования цифровых водяных знаков используется принцип встраивания метки, являющейся узкополосным сигналом, в широком диапазоне частот маркируемого изображения. Указанный метод реализуется при помощи двух различных алгоритмов и их возможных модификаций. В первом случае информация скрывается путем фазовой модуляции информационного сигнала (несущей) с псевдослучайной последовательностью чисел. Во втором — имеющийся диапазон частот делится на несколько каналов и передача производится между этими каналами. Относительно исходного изображения метка является некоторым дополнительным шумом, но так как шум в сигнале присутствует всегда, его незначительное возрастание за счет

внедрения метки не дает заметных на глаз искажений. Кроме того, метка рассеивается по всему исходному изображению, в результате чего становится более устойчивой к вырезанию.

При том повальном воровстве, которое происходит в Internet, польза этой технологии очевидна. Но надо сказать, что на сегодняшний день, несмотря на заявления компаний, разрабатывающих программные продукты для нанесения и считывания цифровых водяных знаков, пока нет ни одного публично известного успешного широкого применения таких технологий. Все водяные знаки оказались нестойкими. Они могут перенести многое — изменение яркости и контраста, использование спецэффектов, даже печать и последующее сканирование, но они не могут перенести хитрое воздействие специальных программ-стирателей, таких как UnZign и StirMark, которые появились в Internet, причем очевидно не с целью насолить фирмам-производителям программ, формирующих водяные знаки, а для того, чтобы дать пользователям возможность сделать правильный выбор, основываясь на независимой оценке стойкости водяных знаков. А оценка эта на сегодняшний день малоутешительна — водяные знаки всех производителей уничтожаются без заметного ухудшения качества изображения соответствующими программами или, на худой конец, «руками».

При использовании всемирной компьютерной сети имеются некоторые особенности применения стеганографии. Онлайновая стеганография основана на том, что для сокрытия информации или переговоров в системе «чат» используются разнообразные веб-сайты и послания настолько неприметные, что никому и в голову не придет искать там чьи-то секреты. С достаточной долей иронии специалисты окрестили эту технику кибер-эквивалентом симпатических чернил.

В качестве «почтовых ящиков» используются совершенно обычные фотогалереи, музыкальные и спортивные сайты, Internet-аукционы, и даже чат-комнаты порнографических сайтов.

По мнению специалистов, используя столь «нехитрую технику», террористы использовали стеганографию для координации своих атак на Нью-Йорк и Вашингтон. «Я могу предположить, что она использовалась», — говорит Нил Ф. Джонсон, специалист по стеганографии в университете Джорджа Мэсона в северной Вирджинии. Используя стеганографию, они умудрялись передавать друг другу карты местностей, диаграммы, важные фотографии и текстовые послания, которые ничем не отличались от тех, что пользователи Internet ежедневно пересылают друг другу в немыслимых количествах. Например, сообщение о том, на какой самолет нужно было сесть в Бостоне, могло быть внесено в изображение футбольной игры в штате Огайо. Кто мог подозревать об этом? Зачастую тайные послания террористов «прятались» в «спаме» — миллионах бесполезных посланий, рассылаемых по адресам электронной почты и практически не регистрируемых 99% пользователей, которые удаляют их из своих почтовых ящиков «не вскрывая».

Правительство США очень обеспокоено использованием террористами стеганографии и учредило проведение исследований по разработке контрмер. Так, WetStone Technologies в Корнинге, Нью-Йорке разрабатывает алгоритм распознавания сообщений, внедренных в цифровые послания. Другой, более примитивный способ обнаружения стеганографических посланий — просматривать Internet-изображения, которые могли затрагивать интересы террористов, такие как фотографии Белого дома или Нью-

Йоркской фондовой биржи. Техника использования стеганографии, например, приводит к смещению в цветовой палитре. «Использование всех существующих стегоинструментов и технологий приводит к некоторым модификациям, — сообщает Джонсон. — Такие изменения создают аномалии. Как если бы голова древнего бегуна обросла светлыми волосами вместо темных»

Характеристика современных стеганографических программ

Существует довольно много программных продуктов, которые применяются для целей стеганографии и реализующих, как правило, средства внедрения секретных данных в графические, звуковые и видеофайлы. Многие из них бесплатны или условно бесплатны (shareware). Пользование большинством из них сводится к нажатию нескольких кнопок в окнах диалога. Достаточно выбрать файл сообщения, который нужно скрыть, затем файл-приемник данных, в котором предполагается скрыть данные (его емкость должна быть достаточна для хранения внедренных данных) и нажать на кнопку OK. Рассмотрим несколько примеров.

StegoDos — одна из свободно распространяемых и широко обсуждаемых программ стеганографии анонимного автора (псевдоним Черный Волк). Представляет собой ряд исполнимых модулей для MS DOS. Работает только с 256-цветными изображениями формата 320x200, которые предварительно должны быть отображены на экране программой просмотра, не входящей в StegoDos. Затем с помощью резидентной программы делается копия видеобуфера компьютера. Полученный образ используется в качестве контейнера, в который помещается закодированное сообщение пользователя. Декодирование производится аналогично — контейнер отображается на экран и вызывается программа извлечения сообщения, которое затем помещается в выходной файл.

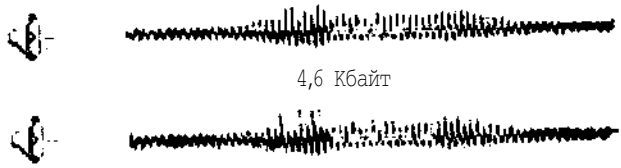
WNS (Белый шумовой шторм — White Noise Storm, автор Arsen Arachelian) — одна из универсальных программ стеганографии для DOS. Автор рекомендует шифровать сообщение перед вложением в контейнер. WNS включает и подпрограмму шифрования, чтобы «рандомизировать» скрывающие биты в контейнере. Программа разработана с использованием результатов спектрального анализа, выгодно отличается качеством сопроводительной документации, что сглаживает некоторое ее отставание в теоретическом отношении. Основной недостаток метода шифрования в WNS — потеря большого количества бит, которые могли бы использоваться в качестве скрывающих. Отсюда — завышенные требования к размерам контейнеров.

S-Tools for Windows v. 3.00 (автор Andy Brown) — один из наиболее развитых универсальных инструментальных комплексов стеганографии. Включает несколько программ, которые обрабатывают изображения GIF и BMP, звуковые WAV-файлы и даже скрывают информацию в «неиспользуемых» областях на гибких дискетах. В дополнение к поддержке 24-битных изображений включает поддержку подпрограмм шифрования (IDEA, MPJ2, DES, 3DES и NSEA) с многочисленными опциями, содержит хороший интерфейс с подсказками и четкую интерактивную документацию.

Работа программы заключается в следующем. Файл-носитель перетаскивается в окно программы, затем в этот файл перетаскивается файл с данными любого формата,

8,9 Кбайт

11,2 Кбайт
(8,9 Кбайт + 2,3 Кбайт текста)



4,6 Кбайт

5,1 Кбайт
(4,6 Кбайт + 0,5 Кбайт текста)

Рис. 5.8. Пример использования программы S-Tools

вводится пароль, выбирается алгоритм шифрования, и перед вами результат, который впечатляет! Внешне графический файл остается практически неизменным, меняются лишь кое-где оттенки цвета. Звуковой файл также не претерпевает заметных изменений. Для большей безопасности следует использовать неизвестные широкой публике изображения, изменения в которых не бросятся в глаза с первого взгляда, а также изображения с большим количеством полутонов и оттенков (пестрые картинки). Для этого подойдет, например, осенний пейзаж, букет цветов и т. п. Рассмотрим один из примеров, представленный на рис. 5.8.

В первом ряду левое изображение (8.9Кбайт) не содержит зашифрованной информации, правое же (11.2Кбайт) содержит небольшой текст, поэтому его конечный размер увеличился. Во втором ряду первый звуковой файл (4.6Кбайт) также «чист», а второй вместил в себя 0.5 Кбайт текста, при этом не увеличив свой размер. Нет практически никаких отличий. Соотношение между размером файла с изображением или звуком и размером текстового файла, который можно спрятать, зависит от конкретного случая. Иногда размер текстового файла даже превышает размер графического. Впрочем, даже если подозрения у кого-то и возникнут, то их придется оставить при себе: не зная пароля, установить сам факт использования S-Tools и тем более доказать это — очень проблематично.

Этому же автору принадлежит интересная реализация GZIP-архиватора. На 100 Кбайт несжатого текста ему удалось добиться включения 1 Кбайта скрытого текста. Специалисты, знакомые с эффективностью (плотностью упаковки) этого архиватора, оценили его весьма высоко.

Covert_TCP 1.0 (автор Craig H. Rowland) предназначен для скрытой передачи файлов по каналам ОС Linux. Эта программа управляет TCP/IP заголовком и передает с каждым файлом один скрытый байт на главную ЭВМ адресата. Программа может работать как станция и как пользователь. При интенсивном трафике возможности передачи скрытых данных весьма велики, тем более, что передача данных производится и со служебными пакетами.

HideSeek v5.0 (программа для DOS) предназначена для обработки gif-файлов. Для рандомизации (но не шифрования) используется алгоритм IDEA. Она работает при различной разрешающей способности дисплея, но может быть довольно медленной для большого gif-файла и/или файла скрываемых данных. Программа свободно распространяется и вполне удобна для знакомства с практическим использованием стеганографии.

Другая распространенная стеганографическая программа — Steganos for Windows95 (shareware). Она обладает практически теми же возможностями, что и S-Tools, но использует другой криптографический алгоритм (HWY1), и, кроме того, способна прятать данные не только в файлах формата bmp и wav, но и в обычных текстовых и HTML-файлах, причем весьма оригинальным способом — в конце каждой строки добавляется определенное число пробелов.

Сегодня на рынке существует довольно много фирм, предлагающих продукты для создания и детектирования водяных знаков. Один из лидеров — фирма Digimarc, программы которой, если верить предоставленной самой фирмой информации, установили себе более миллиона пользователей. Фирма предлагает «скачать» с сайта PictureMarc подключаемый модуль для Photoshop и CorelDraw или выбрать отдельно стоящий ReadMarc.

Единственное, что может противопоставить хакерам компания Digimarc, — это скорость изменения алгоритмов; никаких принципиальных возможностей уберечь метки от акул стегоанализа пока не придумано. Последнее утверждение не так давно было подтверждено комитетом SDMI, объявившим конкурс на взлом собственных технологий защиты музыкальных файлов. Большинство из предложенных технологий было основано на принципах цифровых водяных знаков и, судя по всему, практически все они были взломаны. Другое дело, что качество звука во взломанных файлах представителей SDMI устроило не во всех случаях. Впрочем, можно с определенной долей вероятности предположить, что оно все же было вполне приемлемым — через автоматизированную систему приема вариантов взлома прошло большое количество взломанных с точки зрения потребителя файлов.

Несмотря на молодость компьютерной стеганографии, уже сегодня любой тип данных может быть скрыт и перемещен невидимо в местах, где производится хранение или передача больших объемов цифровых данных,

Создавая определенные удобства для сохранения тайны переписки, стеганография создает условия для возникновения неконтролируемых информационных каналов. В частности, это вызов органам контрразведки, которая неизбежно должна отреагировать новым прорывом в технологиях информационной безопасности. Стеганография — привлекательное средство для деятельности хакеров, она позволяет распространять вирусы. Данный список можно продолжить. Но очевиден тот факт, что прогресс в области стеганографии может кардинально изменить существующие подходы к проблеме информационной безопасности.

В настоящее время компьютерная стеганография продолжает развиваться: формируется теоретическая база, ведется разработка новых, более стойких методов встраивания сообщений. Среди основных причин наблюдающегося всплеска интереса к стеганографии можно выделить принятые в ряде стран ограничения на использование наиболее совершенных методов криптографии, а также проблему защиты авторских прав на художественные произведения в цифровых глобальных сетях. Поэтому в ближайшее время можно ожидать новых публикаций и разработок в этой области.

Хотя стеганография и криптография принципиально отличаются по целям, их не стоит рассматривать как альтернативу друг другу Это, скорее всего, две стороны одной медали. И не только потому, что по-настоящему эффективно лишь их совместное использование, но и потому, что в их основе лежит общая методическая и инструментальная база.

Словарь терминов, определений и сокращений

Abelian group	Абелева группа; абстрактная группа с коммутативной бинарной операцией
Adaptive-chosen-ciphertext	Перебор шифрованного текста; атака методом перебора зашифрованного текста, когда криптоаналитик может перебирать зашифрованные тексты динамически (криптоаналитик может встроить такую атаку в сценарий, когда имеется свободный доступ к части криптографического оборудования, но не известен ключ)
Adaptive-chosen-plaintext	Перебор открытого текста; частный случай атаки методом перебора открытого текста, при котором криптоаналитик имеет возможность перебирать открытые тексты динамически и изменять их или алгоритм их перебора в зависимости от результатов предыдущих шифрований
Adversary	Противник; термин обычно применяется для обозначения противника, нападающего и вообще того, кто желает взломать чью-либо защиту
AES (Advanced Encryption Standard)	Пасширенный стандарт шифрования; стандарт, которым заменяется стандарт DES (Data Encryption Standard - стандарт шифрования данных)
Algebraic attack	Алгебраическая атака; метод криптоаналитической атаки, используемый против зашифрованных блоков, которые предлагают достаточно большой объем математической структуры
Algorithm	Алгоритм; последовательность действий для выполнения задачи
Anonymous FTP (анонимный протокол передачи файлов FTP)	Возможность переноса файлов с удаленного компьютера, соединенного с Internet, без обладания бюджетом на удаленном компьютере. Вместо имени пользователь вводит: «anonymous», а вместо пароля — обычно адрес электронной почты
ANSI (American National Standards Institute)	Американский Институт Национальных Стандартов
API (Application Programming Interface)	Программный интерфейс приложения
Attack	Атака; успешная или неудачная попытка взлома части или всей системы шифрования. См. algebraic attack - алгебраическая атака; birthday attack - атака «по дню рождения»; brute force attack - лобовая атака; chosen ciphertext attack - атака перебором зашифрованного текста; chosen plaintext attack - атака перебором открытого текста; differential cryptanalysis - дифференциальный криптоанализ; known plaintext attack - атака по известному открытому тексту; linear cryptanalysis – линейный криптоанализ; middleperson attack - атака через посредника

Authentication	Аутентификация, установление подлинности; проверка информации о тождестве, монопольном использовании или разрешении
Biometrics	Биометрия; наука об использовании для идентификации личности биологических свойств, например, отпечатков пальцев или голоса
BIOS (Base Input Output System)	Базовая система ввода/вывода
Birthday attack	Атака «по дню рождения»; лобовая атака для выявления коллизий. Получила свое название от парадокса, заключающегося в том, что в группе из 23 человек вероятность совпадения двух или нескольких дней рождений больше чем 50%
Bit	Бит; двоичный символ, принимающий значения 1 или 0
BITNET	Сеть, состоящая из миникомпьютеров, которая объединяет множество учебных заведений (дает возможность посылать электронную почту и передавать файлы, но не позволяет осуществлять удаленный вход)
Blind signature scheme	схема «слепой» подписи; позволяет организовать подписание некоторой стороной сообщения, не разглашая этой стороне никакой содержащейся в сообщении информации (или предоставляя минимум информации)
Block	Блок; последовательность битов, имеющая фиксированную длину; длинные последовательности битов могут быть преобразованы в блоки
Block cipher	Блоковое шифрование; симметричный шифр, при котором сообщение разбивается на блоки и шифруется каждый блок
Block cipher based MAC	MAC (message authentification code - код аутентификации сообщения), получаемый на основе блокового шифрования как функция сжатия ключей
Boolean expression	Булевое выражение; математическое выражение, в котором все переменные имеют значения 0 или 1
Brute force attack	Лобовая атака; атака, подразумевающая перебор всех или значительного количества из всех возможных значений, пока не будет найдено верное; также называется полным перебором
CAPI (Cryptographic Application Programming Interface)	Программный интерфейс криптографического приложения
CCTV	Внутренние системы телевизионного наблюдения
Cecryption	Расшифрование; операция обратная шифрованию
Certificate	Сертификат, свидетельство; в криптографии так называется электронный документ, связывающий вместе некоторые части информации, например, идентификатор пользователя с общим ключом
Certificate revocation list	Список сертификатов, аннулированных до срока их истечения
Certifying Authority (CA)	Персона или организация, создающая сертификаты, свидетельства
Checksum	Контрольная сумма; используется для выявления ошибок; контрольная сумма вычисляется на основе сообщения и передается вместе с сообщением; метод аналогичен проверке на четность

Chosen ciphertext attack	Атака перебором шифрованного текста; атака, при которой криптоаналитик может перебирать шифрованный текст
Chosen plaintext attack	Атака перебором открытого текста; атака, при которой криптоаналитик может перебирать открытый текст, который должен быть зашифрован
Cipher	Шифр; алгоритм шифрования и дешифрования
Ciphertext	Зашифрованный текст; зашифрованные данные
Ciphertext-only attack	Атака только по зашифрованному тексту; способ криптоанализа, когда имеется только некоторый зашифрованный текст и ничего более
CMOS	Энергонезависимая память компьютера, имеет встроенные часы реального времени с календарем, содержит информацию о конфигурации машины
Collision	Коллизия, конфликт; два значения x и y создают (предположительно) коллизию односторонней функции F, если x не равен y, но при этом F (x) = F (y)
Collision search	Поиск коллизии; поиск коллизии для односторонней функции
Collision-free	Бесконфликтность; **хэш-функция** является бесконфликтной, если коллизии сложно обнаружить. Функция является **малоконфликтной,** если сложно рассчитать коллизию для данного сообщения x. То есть невозможно рассчитать сообщение для выражения «y не равен x» таким образом, чтобы H (x) = H (y). Хэш-функция полностью бесконфликтна, если в невозможно рассчитать сообщения для «y не **равен** x» так, чтобы выполнялись условия «y не равен x» и H (x) = H (y)
Commutative	Коммутативный; свойство математической операции, которая возвращает тот же самый результат независимо от порядка обрабатываемых объектов. Например, если a; Ь — целые числа, то a + b = b + a, то есть операция сложения целых чисел коммутативна
Compression function	Функция сжатия; функция, которая сжимает код определенной длины и в более короткий код. См. также hash functions — хэш-**функции**
Compromise	Компрометация; непреднамеренное раскрытие или обнаружение криптографического ключа или кода
COM-файл	Исполняемый модуль, содержащий только бинарный образ задачи без какой-либо управляющей информации; этот тип программ всегда загружается в ОЗУ по одним и тем же адресам (указанным при написании программы)
CRL (Certificate Revocation List)	Список аннулированных сертификатов
Cryptanalysis	Криптоанализ; искусство и наука вскрытия шифра или любой другой формы криптографии
Cryptography	Криптография; искусство и наука защищать информацию средствами математики и обеспечивать высокую степень доверия в области электронных коммуникаций. См. также public key — открытый ключ, secret key — секретный ключ, symmetric-key — симметричный ключ, и threshold cryptography — пороговая криптография
Cryptology	Криптология; ответвление математики, связанное с криптографией и криптоанализом

Cryptosystem	Криптосистема, система шифрования; алгоритм шифрования и расшифровки, в том числе все возможные открытые тексты, зашифрованные тексты и ключи.
DAEMon (Disk And Execution Monitor)	Программа, которая не запускается пользователем или программой пользователя, но дожидается определенных условий, после чего запускается сама
Decryption	Расшифрование; операция обратная шифрованию
DES (Data Encryption Standard)	Стандарт шифрования данных; блоковый шифр, разработанный IBM и правительством США в 70-е годы как официальный стандарт. См. также block cipher — блоковый шифр
Dictionary attack	Атака по словарю; разновидность лобовой атаки, при которой перебираются пароли и/или подключается список заранее созданных значений. Часто применяется как атака предварительного вычисления.
Differential cryptanalysis	Дифференциальный криптоанализ; атака методом перебора открытого текста, основанная на анализе различий между двумя открытыми текстами
Diffie-Hellman key exchange	Обмен ключей по протоколу Diffie-Hellman; протокол обмена ключами, позволяющий участникам договориться по незащищенному каналу об использовании ключей
Digest	Дайджест; обычно используется для описания выхода хэш-функции, например, обзор сообщения описывает шум (хэш) сообщения. При хэшировании входы различной длины сжимаются к заданной длине выхода. Так, например, алгоритм хэширования SHA-1 создает дайджест размером 20 бит независимо от размера входа
Digital envelope	Цифровой конверт; протокол обмена ключами, использующий открытый ключ для шифрования закрытого ключа
Digital fingerprint	Цифровой отпечаток пальца; См. digital signature — цифровая подпись
Digital signature	Цифровая подпись; шифрование обзора сообщения частным ключом
Digital timestamp	Цифровая метка времени; запись, математически связывающая документ со временем и датой
Discrete logarithm	Дискретный логарифм; в группе два элемента d; g таковы, что имеется целое число r, удовлетворяющее условию $g^r = d$; r называется дискретным логарифмом d по основанию g
Discrete logarithm problem	Проблема дискретного логарифма; проблема поиска такого значения r, чтобы $g^r = d$, где d и g - элементы в данной группе. Для некоторых групп поиск дискретного логарифма - сложная проблема, используемая в криптосистеме общего ключа
Distributed key	Распределенный ключ; ключ, который разделен на некоторое количество частей и распределен между различными участниками
DMS (Defense Messaging Service)	Служба защищенной передачи сообщений
DOD (Department of Defense)	Департамент обороны
DSA (Digital Signature Algorithm)	Алгоритм цифровой подписи; метод общего ключа, основанный на проблеме дискретного логарифма

DSS (Digital Signature Standard)	Стандарт цифровой подписи; DSA является стандартом для DSS
ECC (Elliptic Curve Cryptosystem)	Криптосистема Эллиптической Кривой; криптосистема общего ключа, основанная на свойствах эллиптических кривых. Например, структура группы может задана точками эллиптической кривой и для такой группы можно сформулировать проблему дискретного логарифма. Эта проблема считается жесткой и потому может быть использована для криптосистемы
EDP (Electronic Data Processing)	Электронная обработка данных
Electronic mail (e-mail)	Электронная почта; сообщения, посылаемые с помощью электронои связи одним человеком другому по сети Internet
Electronic money	Электронные деньги; электронное математическое представление денег
Elliptic curve	Эллиптическая кривая; набор точек (x; y), удовлетворяющих уравнению формы y 2 = x^3 + ax + b для переменных (x; y), и констант (a;Ь), принадлежащих множеству F, где F - поле
Elliptic curve (factoring) method	Метод разложения на множители эллиптической кривой; специальный алгоритм разложения на множители с целью найти главный фактор p целого числа n методом нахождения эллиптической кривой, количество точек которой, имеющих модуль p, делится только на меньший фактор
Elliptic curve discrete logarithm (ECDL) problem	Проблема дискретного логарифма эллиптической кривой (ECDL); проблема поиска такого значения т, чтобы m*P = Q, где P и Q - две точки на эллиптической кривой
Encryption	Шифрование; преобразование открытого текста в очевидно менее читаемый (называемый зашифрованным текстом) с помощью математических операций. Зашифрованный текст может быть прочтен тем, кто имеет ключ, который расшифровывает зашифрованный текст
Exclusive-OR	См. XOR
EXE-файл	Программный файл (коды модуля, программы), хранящийся на диске, имеющий заголовок и таблицу перемещения. После загрузки модуля в оперативную память, DOS вводит в регистры МП начальные значения (из заголовка) и настраивает программу на выделенные сегменты памяти
Exhaustive search	Полный поиск; при полном поиске проверяется индивидуально каждое значение вплоть до нахождения правильного.
Expiration date	Дата истечения срока; сертификаты и ключи могут иметь ограниченную продолжительность жизни; для контроля используются даты истечения срока
Exponential function	Показательная функция; функция, где переменная находится в показателе степени некоторого ядра, например, b^x, где x - переменная, а Ь> 0 и является некоторой константой
Export encryption	Экспорт шифрования; шифрование в любой форме, которое вывозится из страны-производителя. Например, зашифрованная информация или компьютерный диск, содержащий алгоритмы шифрования, вывозимый из страны

Factor	Фактор, делитель; для любого целого числа n фактором является число, на которое n делится без остатка. Например, 7 - фактор числа 91, потому что результат деления 91 на 7 является целым числом
Factoring	Разложение на множители; разложение целого числа на его главные факторы
FAT	Системная таблица диска, указывающая физическое расположение файлов и свободную область на диске
FBI	ФБР; Федеральное бюро расследований; правительственный правоохранительный орган США
Feistel cipher	Шифр Feistel; специальный класс шифрования с помощью итераций блока, где открытый текст шифруется многократным применением одного и того же преобразования, называемого круглой функцией
Field	Поле; математическая структура, состоящая из конечного или бесконечного набора F и двух бинарных действий, которые называются добавление и мультипликация. Типичные примеры содержат набор вещественных чисел, набор рациональных чисел и набор модуля целых чисел p
FIPS (Federal Information Processing Standards)	Федеральные Стандарты Обработки информации
Flat key space	Набор пространств ключей
FTP (File Transfer Protocol)	Протокол передачи файлов, с помощью которого можно передавать файлы с одного компьютера на другой
Function	Функция; такое математическое отношение между двумя значениями, называемыми вход и выход, что для каждого входа имеется только один выход. Например, f определенное на множестве вещественных чисел как f (x) = x2, есть функция, где входом может быть любое вещественное число x, а выход — квадрат x
Galois field	Поле Галуа; поле с конечным числом элементов. Размер конечного поля должен выражаться простым числом (иметь мощность простого числа)
Generalpurpose factoring algorithm	Общий алгоритм разложения на множители; алгоритм, время выполнения которого зависит только от размера разлагаемого на множители числа
Goppa code	Код Гоппа; класс кодов с исправлением ошибок, используемых в криптосистеме открытого ключа McEliece
Graph	Граф; в математике так называется набор элементов, называемых вершинами или узлами и набор неупорядоченных пар вершин, называемых гранями. Вообще говоря, грань - линия, соединяющая две вершины
GSS-API (generic security service application program interface)	Универсальный защищенный сервис для интерфейса прикладной программы
Hacker	Хакер; персона, пробующая или наносящая вред средствам компьютерной защиты

Handshake	Рукопожатие; протокол, используемый двумя компьютерами для инициализации сеанса связи
Hard problem	Жесткая проблема; проблема, требующая большого объема вычислений, трудная в вычислительном отношении
Hash function	Хэш-функция; функция, которая при различных размерах входа имеет выход фиксированного размера
Identification	Идентификация; процесс устанавления тождества человека или объекта
IEEE (Institute of Electrical and Electronics Engineers)	Институт Инженеров Электричества и Электроники; группа, создающая некоторые стандарты криптографии
IKP (Internet Keyed Payments Protocol)	Протокол защищенных платежей
Import encryption	Импорт шифрования; шифрование, импортированное в страну в любой форме
Internet	Интернет; международная компьютерная сеть передачи данных
ISO (International Standards Organization)	Организация международных эталонов; создает международные эталоны, включая стандарты криптографии
ITU-T (International Telecommunica-tions Union - Telecommunica-tions)	Международное Объединение Передачи данных; сектор стандартизации передачи данных
Key	Ключ; последовательность битов, широко используемая в криптографии для шифрования и расшифровывания данных; также ключ может использоваться для других математических операций. Используя шифр, ключ превращает открытый текст в зашифрованный
Key agreement	Согласование ключей; процесс, используемый двумя или несколькими сторонами, чтобы согласовать секретный симметричный ключ
Key escrow	Процесс, при котором ключи шифрования поддерживаются третьей стороной. Например, ключи шифрования могут предоставляться правительственным агентам или доверителю
Key exchange	обмен ключами; процесс, при котором две стороны обмениваются ключами криптосистемы
Key expansion	Расширение ключа; создание из первоначального ключа другого ключа большего размера
Key generation	Генерация ключа; процесс создания ключа
Key management	Управление ключами; различные процессы, связанные созданием, распределением, установлением подлинности и хранением ключей.
Key pair	Пара ключей; полная информация о ключах криптосистемы; состоит из общего ключа и частного ключа
Key recovery	Восстановление ключа; специальная возможность схемы управления ключами, позволяющая расшифровать сообщение, даже если первоначальный ключ потерян

Key schedule	Расписание ключей; алгоритм, генерирующий дополнительные ключи при блоковом шифровании
Key space	Пространство ключей; множество всех ключей возможных для данной криптосистемы
Knapsack problem	Проблема ранца; проблема выбора из заданного множества определенного набора элементов, общий вес которых будет максимальным, но меньше заданного значения
Known plaintext attack	Атака по известному открытому тексту; форма криптоанализа, когда криптоаналитик знает и открытый текст, и связанный с ним зашифрованный текст
LAN	Локальная вычислительная сеть
LFSR (linear feedback shift register)	Линейный сдвиговый регистр обратной связи. Простая и эффективная математическая модель, позволяющая создавать псевдослучайные последовательности. Используется во многих генераторах ключей для создания последовательностей с необходимыми свойствами
Life cycle	Срок службы; отрезок времени, в течение которого ключ может использоваться и обеспечивать соответствующий уровень защиты
Linear cryptanalysis	Линейный криптоанализ; атака по известному открытому тексту, при которой используются линейные аппроксимации для описания блокового шифрования
Linear key space	Линейное пространство ключей; пространство ключей, где каждый ключ одинаково силен
MAC (message authentication code)	Код идентификации сообщения
Meet-in-the-middle attack	Атака «встреча на середине»; атака по известному открытому тексту против двойного шифрования двумя различными ключами; при этом нападающий шифрует открытый текст одним из ключей и расшифровывает первоначально зашифрованный текст другим ключом, ожидая получить то же самое значение
Message digest	Обзор сообщения; результат применения хэш-функции к сообщению
MHS (Message Handling System)	Система обработки сообщения.
MIME (Multipurpose Internet Mail Extensions)	Формат передачи почтовых сообщений
MIPS (Millions of Instructions Per Second)	Миллионы Команд в Секунду; мера скорости вычислений
MIPS-Year	Год MIPS; количество операций, выполняемых MIPS-машиной за один календарный год.
Network (сеть)	Две и более машин, соединенные вместе с целью обмена данными
NIST (National Institute of Standards)	Национальный Институт Стандартов и Технологии; агентство США, создающее стандарты, связанные с защитой и криптографией (а также другие); эти стандарты издаются как документы FIPS
Nondeterministic	Недетерминированный; не определенный или определяемый предыдущей информацией

Nondeterministic computer	Недетерминированный компьютер; в настоящее время теоретический компьютер, способный выполнять большие объемы вычислений одновременно
Nonlinear key space	Нелинейное пространство ключей; пространство ключей, содержащее сильные и слабые ключи
Non-repudiation	Безвозвратность; свойство системы шифрования. В безвозвратных системах шифрования пользователи не могут отменить выполненные действия
NSA (National Security Agency)	Агентство Национальной безопасности; Правительственное агентство США, занимающнееся декодированием и контролем зарубежных коммуникаций
Number field sieve	Сито поля цифр; метод разложения на множители, в настоящее время самый быстрый универсальный алгоритм разложения на множители
Number theory	Теория чисел; раздел математики, где исследуются отношения и свойства чисел
OAEP (Optimal Asymmetric Encryption Padding)	Гарантированное шифрование сообщения
One-time pad	Разовый ключ; шифрование секретным ключом, где ключ является действительно случайной последовательностью битов, равной по длине сообщению, которое необходимо зашифровать. Шифрование сообщения этим ключом выполняется методом XOR (exclusive-OR). Такое шифрование теоретически не компрометируемо. Поскольку случайные последовательности нельзя использовать повторно, разовый ключ используется в случаях, когда требование защиты информации превышает трудности по дистрибуции разовых ключей, например случайных последовательностей
One-way function	Односторонняя функция; функция, которую легко вычислить в одном направлении, но достаточно трудно вычислить в обратном направлении
One-way hash function	Односторонняя хеш-функция; односторонняя функция, создающая из входной переменной различных размеров выход фиксированного размера
Padding	Заглушка; дополнительные биты, добавляемые к ключу, паролю или открытому тексту шифрованием, что позволяет скрыть их значение
Password	Пароль; строка символов, используемая как ключ доступа к файлу или для шифрования файла
Patent	патент; предоставляемое правительством монопольное право, продавать, использовать изобретение и производить продукт
PKCS (Public-key cryptography Standards)	Стандарты шифрования с открытым ключом; ряд криптографических стандартов, связанных с общими ключами
PKI (Public-key Infrastructure)	Инфраструктура общего ключа. PKI предназначена для решения проблемы управления ключами
Plain text	Открытый текст; данные, которые требуется зашифровать.
Precomputation attack	Атака предварительным вычислением; при такой атаке нападающий заранее рассчитывает таблицу значений, используемых для взлома шифра или пароля

Prime number	Простое число; любое целое число, большее чем 1, которое делится только на 1 и на себя. Первые двенадцать простых чисел: 2,3,5,7,11,13,17,19,23,29,31 и 37
Privacy	Секретность; состояние или качество, изолированности от доступа посторонних
Private key	Секретный ключ; секретный ключ в криптосистеме общего ключа; используется для расшифровки, но также применяется для шифрования вместе с цифровыми подписями
Probabilistic signature scheme (PSS)	Схема вероятностных подписей; гарантирует надежный путь создания подписи с помощью алгоритма RSA
Provably secure	Гарантированная защита; свойство схемы цифровой подписи, когда схема является надежной, если ее защита связана с криптосистемой. Вообще система считается гарантированно защищенной, если на основании некоторых предположений можно математически доказать ее надежность
Public exponent	Общий показатель степени; общий ключ в RSA системе шифрования общим ключом
Public key	Общий ключ; в системе шифрования общим ключом этот ключ доступен всем и используется для шифрования, но также может использоваться для подтверждения подписи
Random number	Случайное число; в отличие от псевдослучайного числа, действительно случайное число, полученное независимо от способов его создания. Для криптографических целей числа, основанные на физических измерениях типа счетчика Гейгера, рассматриваются как случайные
Reduced key space	Сокращенное пространство ключей; при использовании n-разрядного ключа, некоторые действия могут использовать только r < n, в результате чего получается сокращенное пространство ключей
Relatively prime	Относительно простое; два целых числа являются относительно простыми, если они не имеют общих факторов. Например, 14 и 25 относительно простые, в то время как 14 и 91 - нет; так как 7 является их общим фактором
Rounds	Параметр, определяющий, сколько раз функция, называемая круглой функцией, применяется в блоке в шифре Feislel
RSA algorithm	RSA алгоритм; система шифрования общим ключом, основанная на разложении на множители. RSA - Rivest, Shamir Adleman, разработчики системы шифрования общими ключами RSA и основатели RSA Data Security (в настоящее время RSA Security)
Running time	Текущее время; мера времени, требующегося для выполнения специфического алгоритма, являющаяся функцией размера входа
S/MIME (Secure Multipurpose Internet Mail Extensions)	Защищенные многоцелевые расширения почты Internet
S/WAN (Secure Wide Area Network)	Защищенная сеть WAN
Salt	Строка, составленная из случайных (или псевдослучайных) битов, присоединяемая к ключу или паролю, чтобы помешать атаке предварительного вычисления

Secret key	Секретный ключ; в криптографии секретным ключом называется ключ, используемый для шифрования и дешифрования
Secret sharing	Разделение тайны; разделение некоторой тайны, например, секретного ключа на несколько частей таким образом, чтобы из любого заранее указанного количества K частей можно было восстановить тайну, а количества частей K-1 для восстановления тайны не достаточно
Secure channel	Защищенный канал; среда передачи связи, защищенная от перехвата информации и несанкционированного прослушивания
Seed	Обычно случайная последовательность символов, использующаяся для генерации другой, обычно более длинной псевдослучайной последовательности символов
Self-shrinking generator	Генератор с обратной связью, в котором выходной поток Linear Feedback Shift Register (LFSR) можно подать на вход
Self-synchronous	Самосинхронизированный; термин относится к потоковому шифрованию и означает, что поток зашифрованных данных зависит от самих данных и их шифрования
Session key	Ключ сессии; в симметричных криптосистемах ключ, который используется для шифрования только для одного сообщения или для одного сеанса связи
S-HTTP (Secure HyperText Transfer Protocol)	Защищенный гипертекстовый протокол передачи; безопасный способ передачи информации по WWW
Smart card	Смарт-карта; карточка, содержащая компьютерный чип, который используется для хранения или обработки информации
SMTP (Simple Mail Transfer Protocol)	Простой протокол почтовой передачи
SP (указатель вершины стека)	Аппаратный регистр МП, содержащий смещение текущего адреса стека относительно начала стекового сегмента (адрес в регистре SS)
Special-purpose factoring algorithm	Алгоритм разложения на множители специального назначения; алгоритм разложения на множители, который эффективен или неэффективен только для некоторых чисел
SSL (Secure Socket Layer)	Протокол, используемый для безопасной связи Internet
Standards	Условия и протоколы, по которым унифицируются способы связи и фактически вся работа компьютеров
Stream cipher	Потоковое симметричное шифрование на основе секретного ключа; алгоритм шифрования, при котором обрабатывается каждый бит отдельно
Stream cipher based MAC	Потоковый шифр на основе MAC; шифрование, использующее линейные сдвиговые регистры обратной связи (LFSRs) для уменьшения размера обработанных данных
Strong prime	Простое число с некоторыми свойствами, выбранное таким образом, что является недоступным для специальных методов разложения на множители
Subkey	Суб-ключ; значение, генерируемое в процессе работы ключа, используемого в круговом (round) блоковом шифровании
Subset sum problem	Проблема суммы подмножества; проблема, где из заданного множества чисел надо найти подмножество, сумма которого равна заданному значению

Symmetric cipher	Симметричный шифр; алгоритм шифрования, использующий один и тот же ключ для шифрования и расшифрования..
Synchronous	Синхроный; свойство потокового шифрования, означающее, что поток зашифрованных данных сгенерирован независимо от открытого текста и зашифрованного текста.
Tamper resistant	Взломоустойчивый; в криптографии этот термин обычно относится к физическому устройству, которое невозможно или чрезвычайно трудно изменить или извлечь из него информацию.
Telnet	Удаленный доступ, дает возможность абоненту работать на любом компьютере сети Internet как на своем собственном (запускать программы, менять режим работы и т.д.)
Threshold cryptography	Пороговая криптография; разбиение тайны (например, секретного ключа) на части таким образом, что только по некоторым подмножествам п частей можно восстановить тайну.
Trapdoor one-way function	«Лазейка» в односторонней функции; возможность простого обратного вычисления односторонней функций, если вы знаете некоторую секретную информацию. Такая секретная информация называется лазейкой.
Verification	Верификация; процесс сопоставления персоны заявленным о ней данным.
Vernam cipher	Шифр Вернама
WAN (Wide Area Network)	Сеть широкого распространения, которая объединяет между собой компьютеры, находящиеся очень далеко друг от друга, с помощью телефонных линий связи
WATS (Wide Area Telecommunica-tions Service)	Телекоммуникационная служба широкого распространения, позволяет делать удаленные вызовы внутри определенного географического региона, в т.ч. — международные
Weak key	Слабый ключ; ключ, не обеспечивающий достаточного уровня защиты или использующий в шифровании закономерности, которые могут быть взломаны.
Worm («червь»)	Программа, целью которой является бесконечное саморазмножение до полного заполнения дискового пространства
WWW (World Wide Web)	Всемирная Паутина
XOR (сокращение от exclusive-OR)	Бинарный оператор (суммирование по модулю 2), возвращающий в результате 1 , если два значения различны; в противном случае возвращает результат 0.
Zero knowledge proofs	Непроницаемое доказательство знания; доказательство обладания какой-либо информацией, без разглашения этой информации.
Авторизация	Разрешение, передаваемое владельцем, с определенной целью. АО: Передача прав, включая передачу доступа, основанную на правах доступа. ***АО:***Свойство, посредством которого устанавливаются и реализуются права доступа к ресурсам
Администрация безопасности	Должностное лицо, которое устанавливает политику безопасности, а также идентифицирует объекты и участников, к которым применяется политика
Аккредитация	Процедура приемки системы для использования в конкретном окружении

Активная атака	Реализация активной угрозы
Активная угроза	Угроза намеренного несанкционированного изменения состояния системы
Алгоритм аутентификации	Последовательность, связанная с безопасностью информации, которая известна пользователю или содержится в устройстве доступа. Он используется для защищенного доступа к услуге. Могут использоваться сложные алгоритмы
Алгоритм блочного шифрования (n-битный)	Алгоритм блочного шифрования, в котором блоки открытого текста и блоки шифротекста имеют длину n бит. *АО:* Криптографическая система, в которой открытый текст и шифротекст разбиты на блоки
Алгоритм криптографического преобразования	Набор математических правил (определяющих содержание и последовательность операций, зависящих от ключа шифрования) по преобразованию исходного открытого текста к зашифрованному и, наоборот, расшифрованию информации
Алгоритм поточного шифра	Криптографическая система, в которой открытый текст и зашифрованный текст обрабатываются как непрерывный поток
Альтернативное определение	Множество правил, определяющих и ограничивающих виды деятельности объектов и участников, относящиеся к безопасности
Анализ риска	Анализ ресурсов и уязвимости системы для установления ожидаемых потерь в случае определенных событий, основанный на оценках вероятности наступления этих событий
Анализ трафика	Получение информации из наблюдения за потоками трафика (наличие, отсутствие, объем, направление и частота)
Аномалии МП	Специфические особенности выполнения некоторых команд микропроцессора
Анонимность	Принцип, в соответствии с которым чья-либо идентичность скрывается от других сторон
Архитектура безопасности	Архитектура участников и объектов, относящихся к безопасности, и полное множество процедур информации и потоков информации для реализации характеристик безопасности
Асинхронный (asynchronous)	Название множественных программ или процессов, которые перекрывают друг друга в использовании и, возможно, в памяти. Асинхронная атака на систему заключается в том, что одна программа пытается изменить те параметры, которые другая программа проверила на достоверность с положительным результатом, но еще не использовала
Атака (attack)	Попытка злоумышленника обойти систему защиты информационной технологии, вызвать отклонения от нормального протекания инфор-мационного процесса и незаконно воспользоваться ее ресурсами
Атака подбора	Атака на систему аутентификации путем случайного или направленного подбора ее секретных компонент, таких как пароли, Ключи, биометрические пароли, биометрические ключи
Аудит биометрической информации	Регистрация, хранение и обработка результатов биометрической аутентификации за достаточно длинный интервал времени с целью выявления попыток атак на биометрические фрагменты системы защиты
Аутентификатор	Средство аутентификации, представляющее отличительный признак пользователя. Средствами аутентификации пользователя могут быть дополнительные кодовые слова, биометрические данные и другие отличительные признаки пользователя

Аутентификационная информация	Информация, используемая для установления достоверности заявленной идентичности
Аутентификационный запрос	Информация, используемая заявителем для получения обменной аутентификационной информации в целях аутентификации принципала
Аутентификационный маркер	Информация, передаваемая при процедуре сильной аутентификации; может использоваться для аутентификации ее отправителя
Аутентификационный сертификат	Информация в виде сертификата безопасности, который может использоваться для подтверждения идентичности объекта, гарантируемой органом аутентификации
Аутентификация (authentication)	Процесс доказательства и проверки подлинности заявленного элементом информационной технологии имени в рамках заранее определенного протокола. АО: свойство, посредством которого устанавливается правильная идентичность объекта или стороны с требуемой гарантией
Аутентификация источника данных	Подтверждение того, что заявленный источник принятых данных является таковым
Аутентификация объекта	Подтверждение, что заявленный объект является таковым
Аутентификация однорангового объекта	Подтверждение, что взаимодействующий заявленный одноранговый объект является таковым
Аутентификация пользователя	Процесс, разработанный для проверки истинности заявки пользователя относительно своей идентичности. *АО:* Подтверждение подлинности пользователя с помощью предъявляемого им аутентификатора
Аутентификация сообщения	Проверка того, что сообщение было послано неповрежденным, неизмененным и от подразумеваемого отправителя предназначенному получателю
Аутентичность (authenticity)	Свойство данных быть подлинными и свойство систем быть способными обеспечивать подлинность данных. Подлинность данных означает, что они были созданы законными участниками информационного процесса и не подвергались случайным или преднамеренным искажениям. *АО:* Избежание недостатка полноты или точности при санкционированных изменениях информации
Базовые средства управления	Управляющие процедуры, которые образуют минимальные практические уровни защиты
Байт	Единица информации, в системе MS DOS байт может принимать значения кодов от 0 до 255, 2 байта составляют машинное слово (значение от 0 до 65536).
Безопасность	Защита доступности, целостности и конфиденциальности информации. *АО:* Сочетание конфиденциальности, целостности и доступности
Безопасность информации	Состояние защищенности информации, обрабатываемой средствами вычислительной техники или автоматизированной системы от внутренних или внешних угроз. АО: Сочетание конфиденциальности, достоверности, аутентичности, целостности и доступности информации

Биометрическая идентификация	Процесс создания модели, описывающей с заданными значениями ошибок первого и второго рода совокупность биометрических образов конкретной личности в рамках заданного способа наблюдения биометрических образов и в рамках заданного способа измерения контролируемых биометрических параметров. АО; Процесс доказательства и проверки подлинности заявленного пользователем имени, через предъявление пользователем своего биометрического образа и путем преобразования этого образа в соответствии с заранее определенным протоколом аутентификации
Биометрическая система	Техническая система, построенная на измерении биометрических параметров личности, способная после обучения узнавать личность
Биометрический ключ	Ключ, используемый для криптографических преобразований и получаемый из стабильной части измеряемых биометрических параметров личности
Биометрический криптографический процессор	Универсальная программа, имеющая гарантированную стойкость к взлому, способная корректно выполнять под управлением только своего пользователя многообразие различных криптографических операций и в том числе множество общепринятых операций по удаленной криптографической аутентификации, способная адаптироваться к конфигурации используемой вычислительной среды, исправлять ошибки пользователя, кроме того, способная надежно хранить его секреты и с высокой вероятностью узнавать различные варианты биометрии своего конкретного пользователя
Биометрический образ	Непосредственно наблюдаемый системой образ личности без использования, каких либо операций по его предварительной обработке и масштабированию
Биометрический параметр	Параметр личности, легко поддающийся измерению, имеющий достаточную стабильность на прогнозируемый период возможных в будущем измерений, и существенно отличающийся от аналогичных параметров множества других людей. Биометрические параметры получают прямым измерением характерных элементов биометрического образа или путем математических преобразований этого образа
Биометрический пароль	Пароль или парольная фраза, воспроизводимая личностью рукописным способом, с помощью голоса или через использование своего клавиатурного почерка
Биометрический эталон	Данные о стабильной части контролируемых биометрических параметров и их допустимых отклонениях, хранящиеся в биометрической системе для последующего сравнения с ними вновь предъявляемых биометрических образов. Вид эталона определяется принятым в системе решающим правилом
Биометрия	Научная дисциплина, изучающая способы измерения различных параметров человека с целью установления сходства/различий между людьми и выделения одного конкретного человека из множества других людей
Блок (подпрограмма, процедура)	Часть программы (хранящаяся на диске внутри .EXE файла), имеющая собственный набор команд и данных и предназначенная для выполнения некоторых действий с последующей передачей управления тому блоку основной программы, который ее вызвал
Блок криптоалгоритма (cryptographic block)	Порция данных фиксированного для заданного криптоалгоритма размера, преобразуемая им за цикл его работы

16 Зак. 199

Бод (Trapdoor baud, back door)	Единица скорости передачи информации — импульс/секунду, причем импульсы равны по амплитуде. Один бод равняется одному биту в секунду
Брешь в безопасности	Несанкционированное раскрытие, изменение или изъятие информации
Вектор инициализации	Случайное число, которое регулярно обновляется, передается по каналу управления и используется для инициализации алгоритма шифрования
Верительные данные	Данные, передаваемые для установления заявленной идентичности объекта
Весовые коэффициенты нейрона (нейровеса)	Весовые коэффициенты, взвешивающие входные данные нейрона, подбираются или вычисляются при настройке нейрона
Вирус	Фрагмент кода, который копирует себя в другую программу, известную также как "главная программа", модифицируя ее при этом. Вирус не является независимой программой и выполняется только при запуске главной программы. Он дублирует себя, заражая другие программы и вызывая непредсказуемое поведение или повреждение данных и/или программ
Вычислительная неосуществи-мость, вычисли-тельная невозможность	Невозможность выполнить определенное преобразование данных с использованием имеющихся на сегодняшний день или предполагаемых к появлению в не очень отделенном будущем вычислительных средств за разумное время
Вычислительно необратимая функция (one-way function)	Функция, легко вычислимая в прямом направлении, в то время как определение значения ее аргумента при известном значении самой функции вычислительно неосуществимо. Вычисление обратного значения для хорошо спроектированной вычислительно необратимой функции невозможно более эффективным способом, чем перебором по множеству возможных значений ее аргумента (синоним: односторонняя функция)
Гамма (gamma).	Псевдослучайная числовая последовательность, вырабатываемая по заданному алгоритму и используемая для зашифрования открытых данных и расшифрования зашифрованных
Гамма шифра	Псевдослучайная двоичная последовательность, вырабатываемая по заданному алгоритму для зашифровывания открытой информации и расшифровывания зашифрованной
Гаммирование	Процесс наложения по определенному закону гаммы шифра на открытые данные для их зашифрования
Гарантия	Доверие, основанное на некоторой форме анализа, к тому, что цель или требование, либо множество целей и/или требований, выполняется/будет выполнено. *АО:* Доверие к безопасности, обеспечиваемой предметом оценки
Генератор ключей	Тип криптографического оборудования, используемый для выработки криптографических ключей и, при необходимости, векторов инициализации
Гриф секретности	Определенный уровень в конечном множестве иерархических уровней, на котором, по мнению владельца информации, должна размещаться часть чувствительной информации

Двойной контроль	Процесс использования двух или более отдельных совместно действующих объектов (обычно, людей) для защиты чувствительных функций информации в случае, когда одно лицо не имеет доступа или не может использовать материалы, например, криптографический ключ
Действующая привилегия	Привилегия, которая в текущий момент может использоваться процессом. Система принимает во внимание только действующие привилегии при осуществлении контроля доступа и принятии других решений, связанных с политикой безопасности
Дешифрование (deciphering)	Получение открытых данных по зашифрованным в условиях, когда алгоритм расшифрования не является полностью (вместе со всеми секретными параметрами) известным и расшифрование не может быть выполнено обычным путем. Дешифрование шифротекстов является одной из задач криптоаналитика
Дизассемблер	Программа, позволяющая получить текст других программ на языке ассемблер
Динамический биометрический образ	Биометрический образ, который аутентифицируемая личность может изменить по своему желанию, например, сменив воспроизводимое рукописно слово — пароль
Динамический биометрический параметр	Биометрический параметр, получаемый из динамического биометрического образа, который аутентифицируемая личность может изменить по своему желанию, например, сменив воспроизводимое рукописно слово — пароль
Дисперсия	Мера рассеяния значений случайной величины около ее математического ожидания
Доверенная третья сторона	Орган безопасности или его представитель, которому другие объекты доверяют при осуществлении деятельности, связанной с безопасностью. В частности, доверенной третьей стороне доверяет заявитель и/или проверяющий в целях аутентификации
Домен безопасности	Множество объектов и участников, подчиняющихся единой политике безопасности и единой администрации безопасности
Допуск	Атрибут пользователя, разрешающий информационный доступ ко всей чувствительной информации заданного и более низких грифов секретности
Достоверность	Общая точность и полнота информации
Доступ	Способность использовать или вступать в контакт с информацией, либо ресурсами ИТ в информационной системе
Доступ к информации	Ознакомление с информацией, ее обработка, в частности, копирование, модификация или уничтожение информации
Доступ к информации	Способность использовать определенную информацию в рамках информационной системы
Доступность	Избежание неприемлемой задержки в получении санкционированного доступа к информации или ресурсам ИТ. *АО:* Свойство быть доступным и используемым по запросу санкционированного объекта
Доступность информации	Свойство информации, обеспечивающее беспрепятственный доступ к ней для проведения санкционированных операций по ознакомлению, документированию, модификации и уничтожению при ее обработке техническими и/или алгоритмическими средствами. *АО:* Избежание временного или постоянного сокрытия информации от пользователей, получивших права доступа

Драйвер	Резидентная программа, постоянно находящаяся в оперативной памяти и активизирующаяся от соответствующего прерывания, обработка которого за ней закреплена. В отличие от других резидентных программ, драйвер, как правило, создается для сопровождения одного устройства или поддержки одной программы, формируя необходимую для их нормальной работы среду в оперативной памяти
Дублирование информации	Резервная копия информации, которую можно использовать для восстановления
Заверение	Регистрация данных у доверенной третьей стороны, обеспечивающая последующую гарантию точности их характеристик, таких как содержание, время и факт доставки
Заголовок EXE-файла	Начальная часть файла, в которой, в частности, содержится информация о стартовом значении регистров МП, размере всего файла, таблица перемещения и т.д.
Загрузчик ключа	Электронный автономный блок для хранения, по крайней мере, одного криптографического ключа и передачи его по запросу в оборудование
Закрытый ключ ЭЦП	Уникальная последовательность символов, известная обладателю электронной цифровой подписи и предназначенная для создания им с использованием средств ЭЦП электронной цифровой подписи в электронных документах
Зашифрование (encryption, enciphering)	Процесс преобразования открытых данных в зашифрованные при помощи шифра
Защита от НСД	Предотвращение или существенное затруднение НСД
Защитный механизм	Часть исполняемого модуля, реализующая защитные функции: идентификацию пользователя, компьютера, магнитного носителя, защиту программы от исследования и т.п.
Заявитель	Объект, который является принципалом или представляет его от имени этого объекта при аутентификационном обмене. Заявитель выполняет функции, необходимые для обеспечения аутентификационного обмена от имени принципала
Злоумышленник (intruder)	Субъект, оказывающий на информационный процесс воздействия с целью вызвать его отклонение от условий нормального протекания. Злоумышленник идентифицируется набором возможностей по доступу к информационной системе, работу которой он намеревается отклонить от нормы. Считается, что в его распоряжении всегда есть все необходимые для выполнения его задачи технические средства, созданные на данный момент
Идентификатор	Средство идентификации доступа, представляющее собой отличительный признак субъекта. Основным средством идентификации доступа для пользователей является пароль
Идентификационная политика безопасности	Политика безопасности, основанная на идентичностях и/или атрибутах пользователей, группы пользователей или объектов, действующих от имени пользователей, и ресурсов/объектов, к которым осуществляется доступ
Идентификация	Сопоставление предъявленных характеристик с эталонными
Идентификация в узком смысле	Уточнение значений параметров заранее заданной модели с известной структурой, с заданным числом учитываемых параметров, на заданном классе сигналов, при заданных технических ограничениях

Идентификация в широком смысле	Процесс синтеза модели исследуемого объекта, способной его описывать с заданной точностью, включающий выбор используемого математического описания модели, выбор структуры модели, выбор числа учитываемых в модели параметров, выбор тестовых воздействий, определение существующих технических ограничений
Идентификация пользователя	Процесс, с помощью которого система распознает пользователя на основе соответствия более раннему описанию
Идентичность	Уникальный системный признак, применяемый для пользователя
Избыточность	дублирование (критичных) компонентов информационной системы для уменьшения воздействия неисправностей
Имитовставка	Отрезок информации фиксированной длины, полученный по определенному правилу из открытых данных и секретного ключа и добавленный к данным для обеспечения имитозащиты
Имитозащита	Защита систем передачи и хранения информации от навязывания ложных данных. *АО:* Защита системы шифрованной связи от навязывания ложных данных
Инсталляция (Installation)	Установка программного изделия на компьютер (одно из ограничений на программное изделие при его продаже)
Информационная система общего пользования	Информационная система, пользование которой основано на публичном договоре
Информационное взаимодействие или процесс информационного взаимодействия	Обозначают такой процесс взаимодействия двух и более субъектов, основным содержанием которого является передача и/или обработка информации. По большому счету, криптографической может считаться любая функция преобразования данных, секретная сама по себе или зависящая от некоторого секретного параметра
Информация (Information)	Совокупность знаний о фактических данных и зависимостях между ними
Исполняемый модуль	Программа или ее законченная часть (хранящаяся на диске отдельно), имеющая набор команд и данных, имя и предназначенная для загрузки в оперативную память компьютера с последующей передачей ему управления
Исходный текст (исходник)	Текст программы на одном из языков программирования и введенный в компьютер непосредственно программистом (до какой-либо обработки его компьютером)
Канальное шифрование	Индивидуальное использование шифрования данных на каждом канале системы связи
Класс защищенности средств	Определенная совокупность требований по защите средств вычислительной техники и автоматизированных систем от НСД к информации
Класс регистрируемого события	Способ классификации регистрируемых событий по группам на основе типов регистрируемых событий. Тип регистрируемых событий может охватывать несколько классов регистрируемых событий
Класс функциональных возможностей	Предопределенное множество механизмов безопасности, описанных общим образом. *АО:* Предопределенное множество дополнительных функций осуществления безопасности, которое может быть реализовано в предмете оценки

Кластер	Минимальная единица дисковой памяти, выделяемая DOS-ом для хранения файла
Ключ	Конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования информации, обеспечивающее выбор одного преобразования из совокупности всевозможных для данного алгоритма преобразований. АО: Последовательность символов, которая генерируется, хранится, используется и уничтожается в соответствии с криптографическими требованиями и применяется в качестве управляющей информации в криптографических преобразованиях, таких как шифрование/расшифрование, вычисление криптографического чека целостности, генерация/проверка электронной цифровой подписи. АО: Последовательность символов, которая управляет выполнением шифрования и дешифрования
Ключевая (парольная) фраза	Последовательность символов, вводимая пользователем с клавиатуры для его идентификации
Код аутентификации (authentication code)	Имитовставка, код фиксированной длины, вырабатываемый из данных с использованием секретного ключа и добавляемый к данным с целью обнаружения факта изменений хранимых или передаваемых по каналу связи данных
Код аутентификации сообщения	Криптографическая контрольная сумма для обнаружения преднамеренной или случайной модификации данных
Код аутентификации сообщения (КАС)	Поле данных, используемое для проверки аутентичности сообщения
Код обнаружения манипуляций (manipulation detection code)	Код фиксированной длины, вырабатываемый из данных с использованием вычислительно необратимой функции с целью обнаружения факта изменений хранимых или передаваемых по каналу связи данных
Компонент ключа	Один из двух или нескольких параметров, имеющий формат криптографического ключа и объединяемый с одним или несколькими подобными параметрами путем сложения по модулю 2 для формирования криптографического ключа
Конвейер шины данных	Аппаратно реализованная память компьютера, предназначенная для хранения очереди процессорных команд, ожидающих выполнения
Консоль (console)	Операторский терминал, с помощью которого оператор управляет системой
Контрмеры	Услуги безопасности или механизмы, разработанные для противостояния определенной угрозе
Контроллер	Аппаратное устройство, реализующее обмен информации между компьютером и периферийным оборудованием
Контроль (аудит) безопасности	Независимая проверка безопасности информационной системы с определенными целями. *АО:* независимый просмотр и изучение системных записей и действий для проверки адекватности системных средств управления, обеспечения соответствия установленной политике и рабочим процедурам, обнаружения брешей в безопасности и выдачи рекомендаций по изменению управления, политики и процедур

Контроль доступа	Предотвращение несанкционированного использования ресурса, в том числе предотвращение использования ресурса несанкционированным образом
Контроль доступа к информации	Разрешение доступа к информации только полномочным пользователям
Контроль доступа к системе	Разрешение доступа к системе только санкционированным пользователям
Контрольная точка	Команда, после или до выполнения которой может быть зафиксировано состояние вычислительного процесса
Контрольный журнал	Свидетельство, в документальной или другой форме, обеспечивающее проверку функционирования элементов информационной системы. *АО:* Исторические данные и информация, доступные для изучения с целью доказательства правильности и целостности выполнения установленных процедур безопасности, связанных с ключом или транзакцией (транзакциями), и возможности обнаружения брешей в безопасности
Контрольный журнал безопасности	Данные, собираемые и потенциально используемые для облегчения контроля безопасности
Конфиденциальность	Свойство информации, позволяющее при ее передаче, обработке и хранении скрыть ее смысловое содержание, а также делающее доступным смысловое содержание информации только авторизованным пользователям, неодушевленным объектам и процессам. *АО:* Избежание раскрытия информации без разрешения ее владельца. *АО:* Свойство, заключающееся в том, что информация не становится доступной или раскрытой несанкционированным лицам, объектам или процессам
Конфиденциальность информации	Субъективно определяемая характеристика (свойство) информации, составляющая коммерческую или личную тайну
Конфиденциальность потока трафика	Услуга конфиденциальности для защиты от анализа трафика
Корпоративная информационная система	Система, пользователями которой может быть только ограниченный круг лиц, определенный владельцем или соглашением участников корпоративной информационной системы
Корпоративная политика безопасности	Совокупность законов, правил и мероприятий, регулирующих управление, защиту и распределение ресурсов, в том числе чувствительной информации, в пользовательской среде
Коэффициенты линейного предсказания	Коэффициенты линейного цифрового фильтра (рекурсивного или не рекурсивного), специально синтезированного для аппроксимации звуковых волн при возбуждении цифрового фильтра входными импульсами, следующими с периодом основного тона
Кракер (cracker)	Хакер, плохо относящийся к компьютерам, которые взламывает
Криптоанализ (cryptanalysis)	Анализ криптографической системы и/или ее входных и выходных данных для получения конфиденциальных переменнных и/или чувствительных данных, в том числе открытого текста. *АО:* Область знаний о раскрытии шифров (ключей) по имеющемуся зашифрованному тексту
Криптоаналитик (cryptanalyst)	Человек, осуществляющий криптоанализ

Криптование	Словечко, используемое дилетантами вместо стандартного термина шифрование. Настоящие специалисты-криптографы никогда не пользуются этим словом, а также его производными «закриптование», «закриптованные данные», «раскриптование», и т.д.
Криптограф (cryptographer)	Специалист в области криптографии
Криптографическая защита	Защита данных с помощью криптографического преобразования, подразумевающая преобразование данных шифрованием и выработкой имитовставки
Криптографическая защита (cryptographic protection)	Защита информационных процессов от целенаправленных попыток отклонить их от нормальных условий протекания, базирующаяся на криптографических преобразованиях данных
Криптографическая синхронизация	Согласование процесса шифрования и дешифрования
Криптографическая система, криптосистема (cryptographic system, cryptosystem)	Совокупность преобразований открытого текста в шифротекст и наоборот, при чем определенное используемое преобразование (преобразования) выбирается посредством ключей. Преобразования обычно определяются математическим алгоритмом. АО: Совокупность криптоалгоритмов, протоколов и процедур управления ключами. АО: Набор криптографических преобразований или алгоритмов, предназначенных для работы в единой технологической цепочке для решения определенной задачи защиты информационного процесса
Криптографический автомат пользователя	Программа автоматического шифрования/расшифрования файлов данных только конкретного банка, где у пользователя находится его личный счет. Криптографический автомат пользователя создается конкретным банком и настраивается на биометрические параметры только конкретного пользователя, позволяя пользователю упростить работу с банком и отказаться от потенциально опасной операции хранения личных ключей на обычных носителях информации. Понятие — криптографический автомат пользователя — это частный случай более широкого понятия — биометрический криптографический процессор
Криптографический алгоритм (cryptographic algorithm)	Алгоритм преобразования данных, являющийся секретным полностью или частично, или использующий при работе набор секретных параметров. К криптографическим также обычно относят алгоритмы, не являющиеся таковыми в смысле данного выше определения, но работающие с ними в единой технологической цепочке преобразования данных, когда использование одного из них не имеет смысла без использования другого. Примером являются алгоритмы проверки цифровой подписи и зашифрования в асимметричных криптосистемах подписи и шифрования соответственно - они не являются секретными и не используют в работе секретных параметров, но, тем не менее, также считаются криптографическими, так как применяются а единой технологической цепочке вместе с соответствующими алгоритмами формирования цифровой подписи или расшифрования
Криптографический ключ (cryptographic key)	Конкретное секретное значение набора параметров криптографического алгоритма, обеспечивающее выбор одного преобразования из совокупности возможных для данного алгоритма преобразований. **АО:** Параметр, используемый в алгоритме для проверки достоверности, аутентификации, шифрования или дешифрования сообщения

Криптографический протокол	Набор правил и процедур, определяющих использование криптоалгоритма и ключей шифрования
Криптографическое оборудование	Оборудование, в котором выполняются криптографические функции (например, шифрование, аутентификация, генерация ключей)
Криптографическое преобразование	Преобразование данных по криптографическому алгоритму, то есть такое преобразование, часть деталей которого держится в секрете и которое не может быть осуществлено без знания этих деталей
Криптографическое устройство	Блок или узел электронной аппаратуры, реализующий алгоритм шифрования
Криптография (cryptography)	Отрасль знаний, целью которой является изучение и создание криптографических преобразований и алгоритмов. В настоящее время четко различаются две отрасли криптографии: классическая или традиционная криптография и «современная» криптография. *АО:* Научная дисциплина, изучающая принципы, средства и методы преобразования информации с целью скрытия ее информационного содержания, предотвращения ее несанкционированного изменения и/или неавторизованного использования. *АО:* Область знаний, объединяющая принципы, методы и средства преобразования сообщений с целью маскировки содержания информации, невозможности ее искажения и несанкционированного доступа к ней. Достижение указанных целей, как правило, осуществляется шифрованием открытого текста при помощи выбранного ключа
Криптология (cryptology)	Наука, изучающая криптографические преобразования, включает в себя два направления - криптографию и криптоанализ. *АО:* Представляет собой науку, занимающуюся преобразованием информации с целью обеспечения ее секретности
Криптостойкая гамма (strong gamma)	Гамма, по известному фрагменту которой нельзя определить другие ее фрагменты и восстановить со всеми деталями алгоритм, использованный для ее выработки
Криптостойкость, криптографическая стойкость (cryptographic strength)	Устойчивость криптографического алгоритма к его криптоанализу. *АО:* Основная характеристика шифра, определяющая его стойкость к дешифрованию
Лазейка	Скрытый программный или аппаратный механизм, позволяющий обойти системные механизмы защиты. Активизируется некоторым неочевидным способом (например, специальная «случайная» последовательность нажатий на клавиши терминала)
Листинг	Текст программы написанный на одном из языков программирования, в котором, как правило, указана информация по выделенным для программы ресурсам компьютера (распределение памяти и др.) и приведены коды команд. В отличие от исходных текстов, которые вводит программист, листинг — конечный продукт специальных программ (трансляторов, компиляторов, дизассемблеров и т.д.)
Личные данные	Любая информация, связанная с идентифицируемым лицом
Логическая бомба (logic bomb)	Программа, внедренная в прикладную программу; запускается при определенных условиях
Магистральный узел (backbone site)	Ключевой узел USENET и электронной почты, обрабатывающий большое количество поточной информации. Получает и посылает на другие узлы новости и сообщения

Макрос (macro)	Ключевая строка или короткое имя, использующаяся для ссылки на более обширный текст
Маркер	Обменная аутентификационная информация, передаваемая при аутентификационном обмене
Маскарад	Попытка объекта выдать себя за другой объект. *АО:* Нападение на систему, в котором участвует несанкционированный объект, выдающий себя за санкционированный объект с целью получения доступа к системным ресурсам
Математическое ожидание	Характеристика случайной величины, ее определение связано с понятием о среднем значении множества (область центра математического множества)
Мера обеспечения безопасности	Мера, разработанная для предотвращения нарушения безопасности или ограничения его воздействия
Механизм безопасности	Логическая схема или алгоритм, реализующие определенную функцию защиты программно или аппаратно
Мониторинг (текущий контроль)	Непрерывный процесс обнаружения, предназначенный для идентификации характера и времени происшествий или нарушений защиты
МП	Микропроцессор
Муляж	Имитация статического биометрического образа, например изготовление дубликата папиллярного узора пальца
Нарушение безопасности	Событие, при котором компрометируется один или несколько аспектов — доступность, конфиденциальность, целостность и достоверность
Нейрон	Элемент решающего правила или сети, принимающей конечное решение, способный оценивать меру расстояния между контролируемым фрагментом биометрического эталона и предъявленным для сравнения аналогичным фрагментом вектора биометрических параметров
Непризнание участия	Отказ одного из взаимодействующих объектов от факта участия во всех или части процедур взаимодействия
Несанкциониро-ванный	Без определенного разрешения владельца
Несанкциониро-ванный доступ (НСД)	Доступ, осуществляемый с нарушением установленных правил
Несимметричная криптосистема (asymmetric cryptographic system)	Криптосистема, содержащая преобразования (алгоритмы), наборы параметров которых различны и таковы, что по одному из них вычислительно невозможно определить другие. Синонимы: двухключевая криптосистема, криптосистема с открытым ключом
Несимметричный метод аутентификации	Метод демонстрации знания секрета, в котором не каждый из объектов имеет всю аутентификационную информацию
Несимметричный шифр (asymmetric cipher)	Шифр, являющийся несимметричной криптографической системой
НСД	Несанкционированный доступ

НСК	Несанкционированное копирование
Обладатель электронной цифровой подписи	Лицо, на имя которого зарегистрировано право использования электронной цифровой подписи и который обладает соответствующим закрытым ключом ЭЦП, позволяющим с помощью средств ЭЦП создавать свою электронную цифровую подпись *в* электронных документах (подписывать электронные документы)
Обмен данными безопасности	Передача протокольной управляющей информации между открытыми системами как часть работы механизма безопасности
Обнаружение	Установление факта происшествия или нарушения безопасности
Обучающая выборка	Несколько примеров биометрических образов, принадлежащих одной личности и не подвергавшихся какой-либо предварительной обработке, сортировке, прореживанию
Объект безопасности	Пассивный объект, к которому предоставляется или запрещается доступ в соответствии с политикой предоставления полномочий
Объект доступа	Единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа
Ограничение привилегии	Практика предоставления привилегии только на требуемый период для выполнения определенной функции
Односторонняя функция	Математическая функция, которую легко вычислить, но для которой вычислительно сложно найти обращение
Односторонняя хэш-функция (one-way hash function)	Хэш-функция, являющаяся вычислительно необратимой функцией
Оконечное (абонентское) шифрование	Шифрование данных, выполняемое в пределах оконечной системы-источника с соответствующим дешифрованием, выполняемым только в пределах оконечной системы-адресата
Онлайновый (оперативный) аутентификационный сертификат	Особый вид аутентификации, сертифицированный доверенным органом; может использоваться для аутентификации после непосредственного взаимодействия с органом
Орган сертификации	Орган, которому один или несколько пользователей доверяют создание и назначение сертификатов. Дополнительно орган сертификации может создавать ключи пользователей
Отказ в услуге	Воспрепятствование санкционированному доступу к ресурсам, либо задержка, критичная ко времени операций
Открытый ключ (public key)	Несекретный набор параметров асимметричной криптографической системы, необходимый и достаточный для выполнения отдельных криптографических преобразований
Открытый ключ ЭЦП	Уникальная последовательность символов, доступная любому пользователю информационной системы, предназначенная для подтверждения с использованием средств ЭЦП подлинности электронной цифровой подписи в электронном документе
Открытый текст (plain text)	Читаемые данные с доступным семантическим содержанием. *АО:* Массив незашифрованных данных
Отладчик	Программа, позволяющая исследовать процесс выполнения других программ
Отличительный идентификатор	Информация, которая однозначно определяет объект в процессе аутентификации

Оффлайновый (независимый) аутентификационный сертификат	Особый вид аутентификационной информации, связывающий идентичность с криптографическим ключом и сертифицированный доверенным органом; может использоваться без непосредственного взаимодействия с органом
Пароль	Секретная строка символов, используемая при аутентификации пользователя. *АО:* Конфиденциальная аутентификационная информация, состоящая обычно из последовательности символов. АО: Запоминаемая пользователем случайная последовательность символов, являющаяся его секретом и применяемая им в процессе аутентификации. *АО:* Средство идентификации доступа, представляющее собой кодовое слово в буквенной, цифровой или буквенно-цифровой форме, которое вводится в компьютер перед началом диалога с ним с клавиатуры или при помощи идентификационной карты
Парольная фраза	Запоминаемая пользователем фраза из нескольких случайных слов, согласованных между собой по правилам языка пользователя
Пассивная угроза	Угроза несанкционированного раскрытия информации без изменения состояния системы
Пассивное нападение	Реализация пассивной угрозы
Перемешивание (Confusion)	Свойство шифрующего преобразования усложнять взаимосвязи между элементами данных, что затрудняет восстановление функциональных и статистических связей между открытым текстом, ключом и шифротекстом
Переполнение буфера (buffer overflow)	Переполнение происходит, когда в буфер поступает избыточное количество новых данных. Причин может быть две: буфер недостаточно велик, чтобы вместить все данные, которые необходимо, до начала обработки этих данных; либо несоответствие между приемом и обработкой данных
Период основного тона	Период первой форманты звукового фрагмента, эквивалентный интервалу времени между возбуждающими линейный предсказатель входными дельта-импульсами
Персональный идентификационный номер (ПИН)	Это 4 — 12-значный буквенно-цифровой код или пароль, имеющийся у покупателя для аутентификации
ПО	Программное обеспечение
Подделка	Изменение данных сообщения, а также подмена имени (имперсонификация) отправителя. Достоверность сообщения и отправителя можно обеспечить за счет использования надежных идентификационных и криптографических дайджестов сообщений
Подсознательные движения	Хорошо отработанные быстрые движения, выполняемые личностью автоматически без предварительного сознательного анализа производимых в данный момент и будущих действий
Подтверждение подлинности электронной цифровой подписи в электронном документе	Положительный результат подтверждения сертифицированным средством ЭЦП с использованием сертификата ключа подписи принадлежности, содержащейся в электронном документе электронной цифровой подписи ее обладателю и отсутствия искажения и подделки подписанного данной электронной цифровой подписью электронного документа
Политика безопасности	Множество критериев для обеспечения услуг безопасности

Политика защищенного взаимодействия	Общие аспекты политик безопасности, действующих *в* каждом из взаимодействующих приложении и процессе
Пользователь	Легальный пользователь биометрической системы или информационной технологии
Пошаговый режим	Процесс выполнения программы по одной команде. После выполнения каждого шага управление возвращается программе, осуществляющей пошаговый режим (для возможности просмотра состояния ОЗУ и содержимого регистров МП)
Правила разграничения доступа	Совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа
Предмет безопасности	Спецификация безопасности, требуемой от предмета оценки; используется в качестве основы при оценке. Предмет безопасности определяет функции безопасности предмета оценки. Он также может определять цели безопасности, угрозы этим целям и конкретные внедряемые механизмы безопасности
Предмет оценки	Система или продукт, подвергаемый оценке безопасности
Преднамеренная угроза	Угроза, в основе которой лежит злое намерение человека
Прерывание	Программно или аппаратно инициированная передача управления по адресу, который находится в таблице векторов прерываний
Привилегия (полномочие)	Способность осуществлять контролируемую или с ограниченным доступом услугу
Признак привилегии процесса	Каждый процесс в соответствующей системе может иметь несколько связанных с ним признаков привилегий. Состояние данных признаков привилегий определяет, может ли данная привилегия использоваться в текущий момент или контролироваться процессом
Принцип Кирхгофа	Принцип построения криптографических алгоритмов, согласно которому в секрете держится только определенный набор их параметров (ключ), а все остальное может быть открытым без снижения стойкости алгоритма ниже допустимой величины. Был впервые сформулирован в работах голландского криптографа Кирхгофа в списке требований, предъявляемых к практическим шифрам, и единственный из всего списка «дожил» до наших дней ассоциированным с именем автора
Пристыкованный	Блок программы (модуль), который работает только один раз, как правило, сразу после запуска программы, и после передачи управления основной задаче (к которой он пристыкован) в дальнейшем вычислительном процессе не участвует
Проверка достоверности	Процесс проверки целостности сообщения или его отдельных частей
Проверочная аутентификационная информация	Информация, используемая проверяющим для проверки идентичности, заявленной с помощью информации обменной аутентификации
Проверяющий	Объект, который сам является или представляет объект, требующий аутентифицированной идентичности. Проверяющий наделен функциями, необходимыми для выполнения аутентификационных обменов

Происшествие	Событие, которое может представлять осуществление угрозы
Протокол аутентификации	Заранее определенная последовательность действий участников аутентификации, которыми могут быть пользователи, процессы или технические устройства
Протокол криптографический (cryptographic protocol)	Набор правил, регламентирующих использование криптографических преобразований и алгоритмов в информационных процессах
Псевдослучайная последовательность	Последовательность чисел, подчиняющаяся заданному закону распределения
Рабочие процедуры	Совокупность правил, устанавливающих правильное использование предмета оценки
Развертывание ключа (key sheduling)	Алгоритм, позволяющий получить по относительно короткому ключу шифрования последовательность раундовых ключей
Разделение обязанностей	Процедура, которая обеспечивает участие, по крайней мере, двух человек данной организации в любой работе, связанной (в частности) с чувствительной информацией
Разделенное знание	Условие, при котором две или более стороны раздельно и конфиденциально имеют на хранении компоненты одного ключа, которые по отдельности не дают знания результирующего криптографического ключа
Рандомизация (randomisation)	Преобразование исходных данных перед или во время зашифрования с помощью генератора псевдослучайных чисел, имеющее целью скрыть наличие в них идентичных блоков данных
Распределенная безопасность	Безопасность информационной системы, разделенной («распределенной») на две или более взаимосвязанные системы, часто находящиеся в различных географических местоположениях и требующие координированных действий для достижения функциональных требований
Рассеивание (diffusion)	Распространение влияния одного знака открытого текста на много знаков шифротекста, а также распространение влияния одного элемента ключа на много знаков шифротекста
Расшифрование информации (decryption, deciphering)	Процесс преобразования зашифрованных данных в открытые при помощи шифра (этот процесс также называют дешифрованием информации)
Раунд (round)	Один шаг шифрования в шифре Файстеля и близких ему по архитектуре шифрах, в ходе которого одна или несколько частей шифруемого блока данных подвергается модификации
Раундовый ключ (round key, subkey)	Секретный элемент, получаемый из ключа криптоалгоритма и используемый шифром Файстеля и аналогичными криптоалгоритмами на одном раунде шифрования
Регистрационная запись	Дискретный блок данных, записываемый в контрольный журнал при наступлении регистрируемого события. Регистрационная запись состоит из множества регистрационных описаний, каждое из которых имеет ассоциируемые с ним регистрационные атрибуты. Каждая регистрационная запись всегда имеет регистрационное описание заголовка записи и, как правило, дополнительные регистрационные описания субъекта(ов) и объекта(ов), участвующих в событии

Регистрационная поствыборка	Процесс, в ходе которого аудитор выбирает записи из контрольного журнала для анализа. Поствыборка обеспечивает гибкость работы аудитора при выборе записей
Регистрационная предварительная выборка	Процесс, в ходе которого система решает, создавать или нет регистрационную запись при каждом наступлении регистрируемого события. Предварительная выборка предоставляет аудитору средства снижения объема создаваемых регистрационных записей, создавая при этом записи, важные для анализа
Регистрационное описание	Часть регистрационной записи, которая описывает один из субъектов и/или объектов, участвующих в регистрируемом событии
Регистрация работы	Возможность информационной системы, позволяющая отследить в системе действия лиц или идентичностей
Регистрируемое событие	Внутренне обнаруживаемое системой действие, которое может привести к созданию регистрационной записи. Если событие приводит к созданию регистрационной записи (для записи в контрольный журнал) — это «записываемое событие», в противном случае — «незаписываемое событие». Система при обнаружении каждого события решает на основе алгоритма регистрационной предварительной выборки, создавать или нет регистрационную запись. Множество регистрируемых событий определяется системной политикой безопасности
Резидентная программа	Программа, постоянно находящаяся в оперативной памяти и активизирующаяся от соответствующего прерывания, обработка которого за ней закреплена
Рейтинг	Мера гарантии, которая может устанавливаться для предмета оценки; состоит из указания его предмета безопасности, уровня оценки, устанавливаемого путем оценивания правильности его реализации, мнения о его эффективности в контексте существующего или предполагаемого рабочего применения и подтвержденного рейтинга минимальной стойкости механизмов безопасности в контексте этого применения
Риск	Производное от воздействия и опасности. В данном определении как опасность, так и воздействие относятся к одному и тому же определенному сочетанию **«угроза — уязвимость»**. Рассчитанный подобным образом риск для каждого отдельного сочетания «угроза-уязвимость» дает в сумме общий риск. На практике термин «риск» часто используется более упрощенно; при этом используется ограниченный диапазон уровней и для опасности и для воздействия (например, высокий, низкий и средний уровни), что приводит к такому же ограниченному диапазону уровней риска. Риск представляет собой вероятный убыток или возрастание стоимости, являющиеся результатом определенного сочетания "угроза — уязвимость". Данная частная концепция и ее определение наиболее полезны, если можно выполнить надлежащие статистические расчеты на большом объеме данных, обеспечивающем достоверность, например, в страховом деле. Отдельная организация обычно полагается на более простые оценки опасности и воздействия
Самомодифицирующийся модуль	Исполняемый блок программы, изменяющий собственные команды в процессе выполнения
Санкционирование (authorization)	Представление права пользования услугами системы, например, права доступа к данным
Санкционированный доступ к информации	Доступ к информации, не нарушающий правила разграничения доступа

Сегмент	Страница оперативной памяти (блок ОЗУ), отведенная либо для кодов программы (кодовый сегмент), либо под стек (стековый), либо под данные (сегмент данных)
Сегментные регистры	Аппаратные регистры микропроцессора, предназначенные для хранения адресов соответствующих сегментов: CS — кодового, DS — данных, SS — стека; пересылки данных из сегмента в сегмент, в которых участвуют сегментные регистры
Секретность (secrecy)	Свойство данных быть известными и доступными только тому кругу субъектов, для которого они предназначены и свойство криптосистемы обеспечивать секретность защищаемых данных
Секретность данных (Data privacy)	Ограничение, накладываемое автором на доступ к его информации другим лицам. Оформляется присваиванием информации определенного грифа и осуществляется закрытием ее паролем, шифрованием и др. методами
Секретность информации	Характеристика (свойство) информации, определяемая государством (его отдельными органами)
Секретный ключ (secret key)	Набор секретных параметров одного из алгоритмов асимметричной криптосистемы
Сертификат	Открытые ключи пользователя и некоторая другая информация, защищенные от подделки с помощью шифрования на секретном ключе органа сертификации, выпустившего сертификат
Сертификат ключа подписи	Документ на бумажном носителе или электронный документ с электронной цифровой подписью уполномоченного лица удостоверяющего центра, идентифицирующий обладателя электронной цифровой подписи, включающий открытый ключ ЭЦП и выдаваемый удостоверяющим центром пользователю информационной системы для обеспечения возможности подтверждения подлинности электронной цифровой подписи
Сертификационный путь	Упорядоченная последовательность сертификатов объектов в информационном дереве справочника, которую можно обработать совместно с открытым ключом начального объекта пути для получения последнего объекта пути. *АО:* Выпуск формальных заявлений, подтверждающих результаты оценки и правильность использования критериев оценки
Сертификация	Официальная аттестация программы
Сертификация уровня защиты	Процесс установления соответствия средств вычислительной техники или автоматизированных систем набору определенных требований по защите
Сертифицирующее учреждение	Независимая и непредвзятая государственная организация, выполняющая сертификацию
Сеть вычислительная (Net Work)	Система взаимосвязанных между собой компьютеров, а также технического и программного обеспечения для их взаимодействия
Сеть Файстеля (Feistel network)	Архитектура построения блочных шифров, доминирующая в настоящее время в традиционной криптографии, в которой весь процесс шифрования блока выполняется за серию шагов (раундов), на каждом из которых блок делится на изменяемую и постоянную части, с помощью функции шифрования из постоянной части и раундового ключа вырабатывается модифицирующий код, который используется для модификации изменяемой части посредством операции гаммирования. Различают сбалансированную и несбалансированную сети Файстеля (balanced and unbalanced Feistel network). В первой постоянная и изменяемая части имеют одинаковый размер, во второй — разный

Сжатие (compression, reduction)	Устранение избыточности в представлении данных
Сигнатура (signature)	Уникальная характеристика системы, которая может быть проверена
Симметричная криптосистема (symmetric cryptosystem)	Криптографическая система, содержащая преобразования (алгоритмы), выполняемые на одном наборе параметров (ключе) или на различных наборах параметров (ключах) но таким образом, что параметры каждого из преобразований могут быть получены из параметров других преобразований системы
Симметричный шифр (symmetric cipher)	Шифр, являющийся симметричной криптографической системой, то есть использующий для за- и расшифрования один и тот же ключ или такие различные ключи, что по одному из них легко может быть получен другой
Синхропосылка	Открытые параметры алгоритма криптопреобразования, обеспечивающие расшифровывание данных
Система защиты данных (security system)	Комплекс аппаратных, программных и криптографических средств, а также мероприятий, обеспечивающих защиту данных от случайного или преднамеренного разрушения, искажения или использования
Системная политика безопасности	Совокупность законов, правил и практических методов, регулирующих порядок управления, защиты и распределения чувствительной информации и других ресурсов в определенной системе
Скрытый канал	Использование механизма, не предназначенного для передачи данных, с целью пересылки информации способом, нарушающим безопасность
Случайная угроза	Угроза, происхождение которой не является злонамеренным
Смещение ключа, смещение	Процесс сложения по модулю 2 счетчика с ключом
Современная криптография	Раздел криптографии, изучающий и разрабатывающий асимметричные криптографические системы. Синонимы: двухключевая криптография, криптография с открытым ключом
Сообщение	Информация, выраженная в определенной форме и предназначенная для передачи от источника информации к ее получателю с помощью сигналов различной физической природы
Спам	Получение сорных сообщений, борьба с которыми — общая проблема для мира асинхронного обмена сообщениями
Список доступа	Список объектов, имеющих разрешение на доступ к ресурсу, в совокупности с их правами доступа
Средства ЭЦП	Аппаратные и/или программные средства, реализующие хотя бы одну из следующих функций: создание электронной цифровой подписи в электронном документе с использованием закрытого ключа электронной цифровой подписи
Срок безопасности	Временной интервал, в течение которого криптографически защищенные данные имеют ценность
Статический биометрический образ	Биометрический образ личности, который дан ей от рождения и который личность не может изменить по своему желанию, например — папиллярный рисунок пальцев человека
Статический биометрический параметр	Параметр, полученный обработкой статического биометрического образа

Стек	Часть оперативной памяти, выделяемая программе для хранения промежуточных результатов вычислений и данных
Стойкость механизма	Аспект оценивания эффективности предмета оценки, а именно свойство его механизмов безопасности противостоять непосредственному нападению на недостатки в их алгоритмах, принципах и свойствах
Стратегия защиты (security policy)	Формальное определение критериев, особенно оперативных, которыми следует руководствоваться при обеспечении защиты системы от известных угроз
Субъект (subject)	Активный компонент, участник процесса информационного взаимодействия, может быть пользователем (человеком), устройством или компьютерным процессом
Субъект доступа	Лицо или процесс, действие которых регламентируются правилами разграничения доступа
Субъект доступа	Лицо или процесс, осуществляющие доступ к информационному ресурсу с использованием штатных технических средств
Сумма контрольная (control total, checksum)	Информация, предназначенная для проверки правильности записи данных путем подсчета суммы байтов и добавления ее к записи; при считывании данных сумма байтов должна совпасть с контрольной суммой
Сцепление блоков	Шифрование информации таким образом, что каждый блок шифротекста криптографически зависим от предшествующего блока шифротекста
Таблица перемещения	Часть заголовка EXE-файла, содержащая адреса команд и данных в его теле, относительно начала файла на диске. После выделения DOS-ом свободных сегментов для загрузки в ОЗУ, операционная система, пользуясь таблицей перемещений, пересчитает относительные адреса на абсолютные (те, на которых программа реально будет располагаться в оперативной памяти)
Техническая политика безопасности	Совокупность законов, правил и практических методов, регулирующих обработку чувствительной информации и использование ресурсов аппаратным и программным обеспечением системы или продукта (European IT SysITSEC)
Техническая угроза	Угроза, возникающая в результате технологической неисправности за пределами системы
Техническая уязвимость	Уязвимость, возникающая в результате неисправности технологического компонента системы
Точка останова	Адрес команды, перед выполнением которой управление передается отладчику
Точка равновероятных ошибок	Особая точка, при расположении в которой порогового устройства вероятности ошибок первого и второго рода совпадают
Традиционная криптография (traditionnal or conventionnal cryptography)	Раздел криптографии, изучающий и разрабатывающий симметричные криптографические системы. Синонимы: одноключевая криптография, криптография с секретным ключом
Трассировка	Процесс пошагового выполнения программы под отладчиком

Троянский конь	Компьютерная программа с видимо или действительно полезной функцией, которая содержит дополнительные (скрытые) функции, тайно использующие законные полномочия инициирующего процесса в ущерб безопасности. Например, снятие "слепой копии" чувствительного файла для создателя троянского коня
Угроза	Потенциальное действие или событие, которое может привести к нарушению одного или более аспектов безопасности информационной системы. *АО:* Действие или событие, которое может нанести ущерб безопасности. Потенциальное нарушение безопасности
Узел	Самостоятельная машина, соединенная с другими сетью
Управление безопасностью	Управление аспектами безопасности, связанными с управлением сетью и услугами, включая административные, функциональные и эксплуатационные вопросы
Управление ключами	Выработка, хранение, распределение, уничтожение, архивирование и использование ключей в соответствии с политикой безопасности
Управление маршрутизацией	Выполнение правил в процессе маршрутизации с целью выбора или избежания определенных сетей, соединений или коммутационных станций
Уровень полномочий субъекта доступа	Совокупность прав доступа для субъекта доступа
Усилитель (amplifier)	Прибор для увеличения амплитуды сигнала без изменения его свойств
Услуга безопасности	Услуга, предоставляемая уровнем взаимодействующих открытых систем и обеспечивающая надлежащую безопасность систем или передачи данных
Устойчивая к конфликтам	Свойство функции, для которой вычислительно невозможно найти различные входные значения, приводящие к одному и тому же выходному значению
Утилита	Программа, дополняющая операционную систему, выполняющая одну из функций обслуживания компьютера или его периферии.
Уязвимость	Слабое место в информационной системе, которое может привести к нарушению безопасности. *АО:* Слабое место в безопасности предмета оценки ввиду ошибок при анализе, проектировании, внедрении или функционировании
Физическая безопасность	Меры, предпринимаемые для обеспечения физической защиты ресурсов от преднамеренных и случайных угроз
Физическая защита	Устройства и процедуры, разработанные для защиты компонентов информационной системы, а также структуры, в которых они размещаются для защиты от ущерба со стороны физических угроз
Физическая угроза	Угроза, последствия которой приводят к физическому повреждению информационной системы
Фонема	Звуковой аналог соответствующей буквы алфавита
Форманта	Амплитуда одной из кратных гармонических составляющих гласного звукового фрагмента. Форманты имеют номер и их частоты кратны частоте первой форманты или частоте импульсов основного тона
Функция шифрования (encryption function)	Функция, используемая в шифре Файстеля и близких по архитектуре шифрах для выработки кода из постоянной части шифруемого блока и раундового ключа, который используется для модификации преобразуемой части шифруемого блока в одном раунде шифрования

Хэш, хэш-блок, хэш-значение (hash, hash-block, hash-value)	Блок данных фиксированного размера, полученный в результате хэширования массива данных
Хэширование (hashing)	Преобразования массива данных произвольного размера в блок данных фиксированного размера, служащий заменителем исходного массива в некоторых контекстах
Хэш-код	результат применения к битам данных хэш-функции
Хэш-функция (hash-function)	Математическая функция, отображающая значения из (возможно, очень) большого множества значений в меньший диапазон значений. *АО:* Функция, осуществляющая хэширование массива данных
Хэш-функция (хэширование) данных	Математическое преобразование данных, позволяющее сжать информацию до меньшего объема. Различают ключевое и бесключевое хэширование. Вычисление хэш-функции является однонаправленным криптографическим преобразованием без коллизий, не позволяющим восстановить исходные данные
Целостность	Свойство информации, позволяющее сохранять неизменность информации или обнаружить факт ее искажения. ***АО:*** Избежание несанкционированной модификации информации. *АО:* Предотвращение несанкционированной модификации информации
Целостность данных	Свойство, в соответствии с которым данные не были изменены или разрушены несанкционированным образом
Целостность информации	Свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию)
Целостность системы	Свойство, заключающееся в том, что данные и методы обработки данных нельзя изменить или разрушить несанкционированным образом
Центр сертификации ключей	Средства, управляемые органом сертификации, для выработки и возврата сертификатов
Цифровая подпись	Данные, добавляемые к блоку данных, или криптографическое преобразование блока данных, позволяющее получателю блока данных проверить источник и целостность блока данных и защититься от подделки, например, со стороны получателя
Цифровой отпечаток	Характеристика элемента данных, такая как криптографическое контрольное число или результат применения к данным односторонней функции; в значительной степени индивидуальна для элемента данных, при этом вычислительно невозможно найти другой элемент данных, обладающий такой же характеристикой
Червь	Независимая программа, которая воспроизводится путем копирования себя из одного компьютера в другой, как правило, в сети. Отличается от вируса тем, что не портит данные/программы и не вызывает непредсказуемого поведения, однако может вызвать неоправданную загрузку каналов связи и памяти
Чувствительная информация	Информация, несанкционированное раскрытие, модификация или сокрытие которой может привести к ощутимому убытку или ущербу для кого-то или для чего-то
Чувствительность	Мера важности, приписываемая чувствительной информации ее владельцем для указания необходимости в защите. АО: Характеристика ресурса, обозначающая его ценность или важность, в том числе его уязвимость

Шифр	Совокупность обратимых преобразований множества возможных открытых данных на множество возможных зашифрованных данных, осуществляемых по определенным правилам с применением ключа
Шифр (cipher, cypher)	Совокупность алгоритмов криптографических преобразований, отображающих множество возможных открытых данных на множество возможных зашифрованных данных, и обратных им преобразований
Шифр абсолютно стойкий (unbreakable cipher)	Шифр, в котором знание шифротекста не позволяет улучшить оценку соответствующего открытого текста, для абсолютно стойкого шифра дешифрование не имеет практического смысла так как по вероятности успеха ничем не лучше простого угадывания открытого текста *в* отсутствии каких-либо дополнительных данных. Синонимы: невскрываемый, совершенный шифр
Шифр аддитивный (additive cipher)	Шифр гаммирования, в котором для наложения гаммы на данные используется бинарная операция аддитивного типа
Шифр блочный (block cipher)	Шифр, в котором данные шифруются порциями одинакового размера, называемыми блоками, и результат зашифрования очередного блока зависит только от значения этого блока и от значения ключа шифрования, и не зависит от расположения блока в шифруемом массиве и от других блоков массива
Шифр гаммирования	Потоковый шифр, в котором для зашифрования данных используется гаммирование
Шифр замены (substitution cipher)	Шифр, в котором отдельные символы исходного текста или их группы заменяются на другие символы или группы символов, сохраняя при этом свое положение в тексте относительно других заменяемых групп
Шифр несовершенный (breakable cipher)	Шифр, не являющийся абсолютно стойким
Шифр перестановки (permutation cipher)	Шифр, в котором процедура зашифрования заключается в перестановках элементов исходного текста или их групп, сами элементы при этом остаются неизменными
Шифр потоковый или поточный (stream cipher, general stream cipher)	Шифр, в котором результат зашифрования очередной порции данных зависит от самой этой порции и от всех предыдущих данных шифруемого массива, в важном частном случае он зависит от самой порции данных и от ее позиции в массиве и не зависит от значения предшествующих и последующих порций данных. Иногда данное условие дополняют требованием, что за один шаг шифруется элементарная структурная единица данных — бит, символ текста или байт. В зарубежной литературе потоковые без учета этого, последнего, требования, шифры называют общими потоковыми шифрами (general stream cipher), а с учетом — просто потоковыми шифрами (stream cipher)
Шифр составной (product cipher)	Шифр, составленный из нескольких более простых шифров, которые используются *в* определенной последовательности при зашифровании и расшифровании данных, обычно составные шифры строятся из большого числа элементарных шифров, каждый из которых заключается в элементарном преобразовании данных
Шифр Файстеля (Feistel cipher)	Шифр, построенный в соответствии с архитектурой сети Файстеля

Шифрование (enciphering/deciphering and encryption/decryption)	Криптографическое преобразование данных для получения шифротекста. *АО:* Процесс шифрования или расшифрования
Шифрование информации	Процесс преобразования открытых данных в зашифрованные с помощью шифра. Иногда этот процесс называют зашифрованием информации. Шифрование является преобразованием сообщения по определенным правилам, что делает его бессмысленным набором знаков для непосвященного в тайну шифра человека
Шифротекст (ciphertext)	Данные, полученные в результате шифрования. Семантическое содержание полученных данных недоступно. *АО:* Массив зашифрованных данных, то есть данных, подвергнутых процедуре зашифрования
Электронная доска объявлений BBS (Bulletin Board System)	Компьютер, установленный на прием вызовов с модема. Пользователи устанавливают с ним связь и получают доступ к различным услугам, включая электронную почту, обмен сообщениями, игры и т. д.
Электронная цифровая подпись (ЭЦП)	Специально созданный файл (signature), который представляет собой текстовую подпись. Она представляет собой совокупность данных в электронной форме, которые безошибочно ассоциируются с каким-либо электронным документом, позволяющее идентифицировать его автора
Электронная цифровая подпись (ЭЦП)	Данные, приписываемые к информации, или криптографическое преобразование информации, позволяющие получателю информации убедиться в ее целостности и подлинности источника информации, а отправителю — защитить информацию от подделки, например, получателем
Электронные деньги	Электронные аналоги денег, чековых книжек, ценных бумаг, выпущенные в обращение банком и обеспеченные активами банка эмитента
Электронные монеты	Файлы, созданные банком и имеющие стоимость кратную принятой единице оплаты (аналог обычных монет). Подлинность электронных монет общедоступна для проверки, например, путем проверки электронной цифровой подписи банка их выпустившего. Процедура оплаты производится путем пересылки файла электронной монеты от покупателя к продавцу. Покупатель не имеет возможности повторно воспользоваться однажды использованным файлом электронной монеты
Электронный документ	Документ, в котором информация представлена в электронно-цифровой форме
Элемент оглавления	Структура, описывающая дисковый файл
Эмитент	Учреждение, которое выпускает карточки для их владельцев; отвечает за общий файл данных и распределение файлов прикладных данных
Эмулятор	Устройство (программа), позволяющее анализировать результаты выполнения каждой команды исследуемой программы без реальной передачи ей управления
Язык заявок	Ограниченное подмножество естественного языка, применяемое для снижения неоднозначности при описании потребности в мерах обеспечения защиты и их заявленных функциональных возможностей

ЛИТЕРАТУРА

Алексеенко В.Н., Сокольский Б.Е. Система защиты коммерческих объектов.//Технические средства защиты.— М., 1992.

Американская армия готовится к кибервойне. Служба новостей Ростов.ру. 27.11.2000

Ананьев Виктор. Электронная тайнопись. // Магия ПК. № 10, 1998.

Андрианов В. И., Бородин В. А., Соколов А. В. «Шпионские штучки» и устройства для защиты объектов и информации. — СПб.: Лань, 1996. — 272 с.

Андрианов В. И., Соколов А. В. «Шпионские штучки», или Как сберечь свои секреты. — СПб.: Полигон, 1997. — 272 с.

Андрианов В. И., Соколов А. В. Средства мобильной связи. — СПб.: BHV-Санкт-Петербург, 1998. — 256 с.

Андрианов В. И., Соколов А. В. Устройства для защиты объектов и информации. («Шпионские штучки») — М.: ООО «Фирма «Издательство АСТ»; ООО «Издательство «Полигон», 2000. — 256 с.

Андрианов В. И., Соколов А. В. Охранные системы для дома и офиса. Спб.: БХВ-Петербург; Арлит., 2002. — 304 с.: ил. — (Техника в вашем доме).

Анин Б. Ю. Защита компьютерной информации. — СПб.: BHV-Санкт-Петербург, 2000. — 384 с.

Анциферов Алексей. Канадские хакеры атакуют американские сервера. // Сервер Компьютерных Новостей (http://computer-news.ru) —31.03.2000.

Атражев М. П. и др. Борьба с радиоэлектронными средствами.— М.: Воениздат, 1972.—272с.

Ахмед Н., Рао К. Р. Ортогональные преобразования при обработке цифровых сигналов. — М.: Связь, 1980. — 248с.

Баранов В. М. и др. Защита информации в системах и средствах информатизации и связи. / Учеб. пособие — СПб.: 1996. — 111 с.

Барсуков В. С., Водолазский В. В. «Интегральная безопасность информационно-вычислительных и телекоммуникационных сетей». Технологии электронных коммуникаций. Т. 34, т. 35.— М.: 1992.

Барсуков В. С., Дворянкин С. В., Шеремет И. А. Безопасность связи в каналах телекоммуникаций — М.: НИФ «Электронные знания», 1992.

Барсуков В.С., Романцов А.П. Компьютерная стеганография вчера, сегодня, завтра. //http://www.bnti.ru/dbtexts/analmat/stegan/

Барсуков Вячеслав. Защита компьютерных систем от силовых деструктивных воздействий. // Jet info № 2(81) 2000. http://www.jetinfo.ru/2000/2/2/article2.2.2000519.html.

Батурин Ю. М., Жодзишский А. М. Компьютерная преступность и компьютерная безопасность. — М.: Юрид. лит., 1991. — 160 с.

Батурин Ю. М., Жодзишский А. М. Компьютерная преступность и компьютерная безопасность.— М.: Юрид. лит., 1991. —160с.

Безруков Н. Н. Компьютерная вирусология: Справ, руководство. — К.: УРЕ, 1991. — 416с.

Безруков Н. Н. Компьютерные вирусы. Ц М..: Наука, 1991.

Беляев А. В. Победитель AES — шифр Rijndael. http://www.creativeport.ru/internet/infsecure/index.html

Бержье Ж. Промышленный шпионаж.— М.: Международные отношения, 1972.

Бертсекас Д., Галлагер Р. Сети передачи данных. — М.: Мир, 1989. — 542 с;. Бизнес и безопасность.— М.: КМЦ «Центурион», 1992,

Блачарски Дэн. Наведение порядка в политике защиты. // LAN/Журнал сетевых решений. — Сентябрь 2000.

Борейко Александр. Получи и распишись. // Ведомости, 21 июня 200 г. — www.vedomosti.ru

Бояров А. Г. Технология идентификация личности по произвольной слитной речи. http://conf.mitme.ru/articles/261.html

Бриккелл Ф. Э., Одлижко Э. М. Криптоанализ: Обзор новейших результатов. — ТИИЭР, 1988, т. 76, № 5.

Быков С. Ф. Алгоритм сжатия JPEG с позиции компьютерной стеганографии. // Защита информации. Конфидент, № 3, 2000, стр. 26.

Вакин С. А., Шустов Л. Н. Основы радиопротиводействия радиотехнической разведке. М.: Сов. Радио. 1968.

Варакин Л. Е. Интеллектуальная сеть: концепция и архитектура. // Электросвязь, 1992.—№ 1.

Вартанесян В. А. Радиоэлектронная разведка. М.: Воениздат, 1991. —255с.

Василенко В. Нахождение неисправностей в блоке питания IBM PC AT. //Радиолюбитель. Ваш компьютер. № 8, 1999.http://spirin.narod.ru/

Винокуров А. ГОСТ не прост, а очень прост! — Монитор, № 1, 1995.

Винокуров Андрей. Криптография, ее истоки и место в современном обществе. http//security.nsys.by/, http://www.enlight.ru/crypto/

Винокуров Андрей. Криптография. Сравнение возможностей различных алгоритмов. Проблема выбора. http//security.nsys.by/, http://www.enlight.ru/crypto/

Вишняков С. М. Нормативное обеспечение оценки устойчивости к электромагнитным помехам средств и систем контроля и управления доступом. // Системы безопасности, апрель—май 2001.

Владов Е., Хромов И. Мир и безопасность в России до 2010 года. Попытка прогноза. // http://www.dol.ru/users/secur/vitmib79.htm

Волин М. Л. Паразитные связи и наводки.— М.: Сов. радио, 1965. — 296 с.

Восприятие информации в системах искусственного интеллекта: Учеб. пособие / В. М. Игнатьев, Е. В. Ларкин. Тул. гос. техн. ун-т: Тула, 1993. — 88 с.

Гавриш В. Практическое пособие по защите коммерческой тайны, Симферополь, «Таврида», 1994.

Гайкович В. Ю., Ершов Д. В. Основы безопасности информационных технологий. — М.: МИФИ, 1995. — 365с.

Галлагер Р. Теория информации и надежная связь. — М.: Сов. радио, 1974. — 534 с.

Генне О. В. Основные положения стеганографии. // Защита информации. Конфидент. № 3, 2000

Герасименко В. А. Защита информации в АСОД./в двух частях.—М.: Энергоатомиздат, 1994.

Герасименко В. А., Размахнин М. К. Криптографические методы в автоматизированных системах. // Зарубежная радиоэлектроника. 1982. № 8. — С. 97—124.

Голиков И., Казанцев Т. Ключи вам больше не нужны. http://www.securityclub.ru/bisec/journal18/acd_serv.htm

ГОСТ 2847-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. — 10с.

Гриняев С. Н. Информационный терроризм: предпосылки и возможные последствия. // http://www.e-journal.ru/p_besop-st19.html.

Гроувер Д. и др. Защита программного обеспечения. — М.: Мир, 1992.

Гурвич И. С. Защита ЭВМ от внешних помех.— М.: Энергоатомиздат, 1984.

Гуриев Владимир. Между строк. http://www.computerra.tomsk.ru/arc38_2.shtml.

Гушер А.И. Социально-правовые аспекты терроризма. // http://www.cssfund.ru/Art00021.html.

Давыдовский А. И., Максимов В. А. Введение в защиту информации. Интеркомпьютер, 1990.— № 1.

Данилюк Владимир. Закодированные послания. http://www.nalogi.net/crimenal/2001/crim01 10_01.1.htm.

Дебора Редклифф. Цифровая подпись. // Еженедельник «Computerworld Россия» 10.05.2000.

Дебора Рэдклифф. Хроника хакерской атаки. // Сети, февраль 2000.

Девид Легард. Неудачная архитектура — находка для хакера. // Еженедельник «Computerworld Россия» 21.03.2000.

Джек Маккарти. ЦРУ опасается кибератак. // Еженедельник «Computerworld Россия» №10, 2000.

Джон Вакка. Секреты безопасности в Internet. Киев, «Диалектика», 1997. — 506 с.

Джоул Снайдер. Защищая «последнюю милю». // Сети, февраль 2000.

Диффи У Первые десять лет шифрования с открытым ключом//ТИИЭР, т. 76,1988. — № 5.— С. 55—74.

Диффи У., Хелман Н. Защищенность и имитостойкость: введение в криптографию //ТИИЭР, т. 67,1979.—№ 3.—С. 71—109.

Дэвид Стенг, Сильвия Муи. Секреты безопасности сетей. Киев, «Диалектика», ИнфОрмейшн Компьютер Энтерпрайз, 1996. — 544 с.

Елисеев Игорь. Что не ГОСТ — то не защита? // Еженедельник «Computerworld Россия» 14.03.2000.

Ефимов А., Кузнецов П., Лукашин А. Проблемы безопасности программного обеспечения критических систем.

Жельников В. Криптография от папируса до компьютера. — М.:ABF, 1997. — 336 с.

Женило В.Р. Компьютерная фоноскопия. М.: Типография Академии МВД России, 1995, 208 с.

Завадский И.И. Информационная война — что это такое? // http://www.fbr.donetsk.ua/InfoWar/.

Замарин А., Андреев А., Ковалевский В. Битва за информацию. Стратегия защиты. // Безопасность. Достоверность. Информация. — 1995, № 2. — С. 21—23.

Замарин А., Андреев А., Ковалевский В., Белоглядов И. Атака на текст: криптограф против аналитика. // Безопасность. Достоверность. Информация. — 1995, № 3. — С. 20—22.

Запечников С. В. Сравнительная оценка современных методов анализа безопасности многосторонних криптографических протоколов. Москва. МИФИ. http://www.tsure.ru:8101/Univercity/Facultties/Fib/bit/rus/sem2001/84.html

Захаров Л. Ф. Современная концепция построения систем электропитания. http://st.ess.ru/publications/

Защита государственных и промышленных секретов. Методы обнаружения вторжений в вычислительные системы. // Ин. печать об экономическом, научно-техническом и военном потенциале государств — участников СНГ и технических средств его выявления. Серия — Технические средства разведывательных служб капиталистических государств. ВИНИТИ, 1993, № 7. — С. 8—15.

Защита данных в информационно- вычислительных сетях. Под ред. Ронжина А. А. — М.: ИНКО «КАМИ», 1991.—128 с.

Защита информации в компьютерных системах. Под ред. Шмакова Э.М. — СПб.: СПбГТУ, 1993. — 100 с.

Защита программного обеспечения. Под ред. Гроувера Д. Пер. С англ. — М.: МИР, 1992.-285с.

Иванов А.И. Биометрическая идентификация личности по динамике подсознательных движений. Пенза. 2000. http://beda.stup.ac.ru/biometry

Иванов В., Залогин Н. Активная маскировка побочных излучений вычислительных систем. // Компьютер Пресс, 1993. — № 10.

Ивонин М. В. Криптографические протоколы распределения ключей для групп с динамическим составом участников. Декабрь 1999г. http://www.securityportal.ru/cripto/ac.shtml.

Касперский Е. Компьютерные вирусы в MS-DOS. — М.: «ЭДЭЛЬ», 1992. — 176 с.

Каторин Ю. Ф., Куренков Е. В., Лысов А. В., Остапенко А. Н. Энциклопедия промышленного шпионажа.// Антишпионские штучки. — СПб.: Полигон, 1999.—512с.

Кащеев В. И. Мониторинг телефонной сети. // Системы безопасности, 1995. —№ 1.

Кен Филлипс. Биометрия, о которой нельзя забыть. // Компьютерная неделя № 2 (126) — 1998

Киселев А. Е. и др. Коммерческая безопасность.— М.: Инфо Арт, 1993.

Кларк Элизабет. Новое лицо идентификационных устройств. // LAN / Журнал сетевых решений. — Сентябрь 2000.

Ковалевский В. Э., Максимов В. А. Криптографические методы // Компьютер Пресс: 1993.— № 5.— С, 31—34.

Коновалов Д. Н., Бояров А. Г. Технология защиты информации на основе идентификации голоса. http://www.fact.ru/archive/07/voice.shtml

Корецкий А. На смену ядерной бомбе пришла информация. // http://www.internews.ru/~rbn/637902.html.

Корт Семен. Современные методы борьбы с компьютерными вирусами.// Банковское дело в Москве. http://www.bdm.ru

Криптографический ликбез. http://www.racal.ru/rsp/eliptic_curve_cryptography.htm

Криптографические методы защиты информации в локальных вычислительных сетях. Под общей редакцией Дружинина А.В., Замарина А.И., Максимова Ю.Н. ВИККА им. А.Ф. Можайского, 1998. — 194 с.

Круглов В. Какой будет вооруженная борьба в будущем? http://www.nasledie.ru/oboz/N08_00/08_13.HTM

Кузнецов П.А. Информационная война и бизнес. // http://www.fbr.donetsk.ua/InfoWar/.

Кустов В. Н., А. А. Федчук. Методы встраивания скрытых сообщений. // Защита информации. Конфидент, № 3, 2000, стр. 34.

Лебедев Анатолий. Криптография и компьютерная безопасность. http//security.nsys.by/

Лебедев Валерий. Радость хакера. http://www.lebed.com/

Левиков В. Я. Проблемы возможности заражения компьютерными вирусами персональных компьютеров, работающих в сети Интернет. http://ims98.nw.ru/cgi-bin

Лесли Гофф. Червь выключает сеть. // Еженедельник «Computerworld Россия» 27.06. 2000.

Ли Коупленд. На аукционах торгуют ворованным. // Еженедельник «Computerworld Россия» 10.05.2000.

Лысов А. В., Остапенко А. Н. Промышленный шпионаж в России: методы и средства.— СПб., Бум Техно, 1994.

Лысов А. В., Остапенко А. Н. Телефон и безопасность.— СПб., Лаборатория ППШ, 1995.

Месса Л. Введение в современную криптографию// ТИИЭР, т. 76, 1988. — № 5. — С. 24—42,

Максимов Ю. Н. и др. Организационно-технические методы контроля защиты информации в объектах ЭВТ: Учебное пособие. — СПб.: ВИККА, 1994. — 77 с.

Медведковский И. Д., Семьянов П. В. Атака через «INTERNET». СПб.НПО «Мир и семья — 95», 1997. — 280 с.

Межутков А., Мяснянкин В. Электронная подпись, или Тернистый путь избавления от бумаги. // Системы безопасности № 40, август—сентябрь 2001.

Мельников В. В. Защита информации в компьютерных системах. М., «Финансы и статистика», 1997. — 364 с.

Минаев В. А., Пеньшин И. В., Потанин В. Е., Скрыль С.В. Анализ угроз безопасности информации в информационно-телекоммуникационных системах. http://www.sec.ru/

Миронычев С. Коммерческая разведка и контрразведка, или Промышленный шпионаж в России и методы борьбы с ним. М.: Дружок, 1995.

Михайлов А. С. Измерение параметров ЭМС РЭС.— М.: Связь, 1980.—200 с.

Молдовян Н. А., Молдовяну П.А. Гибкие шифры для защиты информации в сетях ЭВМ. — Спб., Государственный НИИ моделирования и интеллектуализации сложных систем. http://risbank.spb.ru/risbank2/tm98/078.HTM

Морозов И. Л. Проблемы классификации информационного оружия в современной Российской науке. http://morozov.voljsky.ru/library

Наумов А. Алло! Вас подслушивают. // Деловые люди, 1992.

Никулин О. Ю., Петрушин А. Н. Системы телевизионного наблюдения.— М.: «Оберег РБ», 1997.

Новиков А. А. Биометрическая идентификация личности на основе спектрального анализа голоса. Тула. 2000

Овсянников Вячеслав. О правильном «питании». // CHIP—Панорама № 5, 2000. http://epos.kiev.ua/pubs/

Петелин Р. Ю., Петелин Ю. В. Звуковая студия в PC. — СПб.: BHV-Санкт-Петербург, 1998. — 256 с

Плотников В.Н., Суханов В.А., Жигулевцев Ю. И. Речевой диалог в системах управления. — М.:Машиностроение, 1988. — 244с.

Предпринимательство и безопасность / Под ред. Долгополова Ю. Б.—М.: Универсум, 1991.

Применко Э. А., Винокуров А. А. Сравнение стандарта шифрования алгоритма ГОСТ 28147-89 и алгоритма Rijndael. // Системы безопасности, июнь—июль 2001.

Проскурин В. Г. Перехватчики паролей пользователей операционных систем http://www.warning.dp.ua

Сапожников М. А. Электроакустика. М,: Связь, 1978.

Прохоров Александр. Мой дом — моя крепость, мое лицо — мой пропуск. http://computer-press.bos.ru/comhress/cp0700/cp2000_07_10.htm

Разумов А., Кадуков А. Банкиры, гоните бабки! Угроза электромагнитного террора. «Новый Петербургъ», № 15(482), 12.04.2001 г.

Ральф Надер. Закон о цифровой подписи должен защищать потребителя. // Еженедельник «Computerworld Россия» 14.03.2000.

Рамишвили Г. С. Автоматическое опознавание говорящего по голосу. — М.: Радио и связь, 1981.—224 с.

Рамишвили Г.С. Автоматическое опознавание говорящего по голосу. — М.: Радио и связь, 1981.—224 с.

Роберт Виберт. Как поймать зловредный код. // LAN/Журнал сетевых решений. — Май 2001.

Сергеев Лев. Компьютерные вирусы: вчера, сегодня, завтра. // http://www.compulog.ru/

Сердюк В.А. Криминализация глобальных информационных сетей: миф или реальность. // Системы безопасности. — сентябрь-октябрь 2000 г.- с.84-87.

Сердюков В. Д. Опознавание речевых сигналов на фоне мешающих факторов. Тбилиси, Наука: 1987, 142 с.

Сердюков В. Д. Опознавание речевых сигналов на фоне мешающих факторов. Тбилиси, Наука: 1987, 142с.

Системы идентификации личности по отпечаткам пальцев. КТЦ «Охранные системы» http://www.magazine.security.com.ua/articles/0503.shtml

Соболев Е. А. Защита в Сети. http://www.softbest.ru

Соболев Е. А. О защите информации. http://www.softbest.ru

Соколов А. В. Шпионские штучки. Новое и лучшее. — СПб.: Полигон, 2000. — 256 с.

Соколов А. В., Степанюк О. М. Методы информационной защиты объектов и компьютерных сетей. (Серия «Шпионские штучки»). — СПб.: Полигон, 2000. — 272 с.

Статистические методы для ЭВМ / Под ред. К. Энслейна, Э. Рэл-стона, Г. С. Уилфа: пер. с англ. / Под ред. М. Б. Малютова. — М.: Наука. Гл. ред. физ.-мат. лит., 1986. — 464 с.

Стеганография в компьютерном исполнении — средство террористов для обмена информацией. http://infosci.narod.ru/news/011010-6.html (11 октября 2001 г.).

Стеганография. http://itt.com.ua/win/1999/steganog.htm.

Стив Александер. Вирусы, черви, троянские кони и зомби. // Еженедельник «Computerworld Россия» 23.05.2001.

Судов Евгений. О политике и экономике антивирусной защиты. // «Мой Компьютерный журнал» http://www.compulog.ru

Терминология в области защиты информации. Справочник. — М.: ВНИИ стандарт, 1993. —49 с.

Технические средства разведки. / Под ред. В. И. Мухина. — М., РВСН, 1992. Технический шпионаж и борьба с ним. Минск. ТГО, 1993,

Технические средства разведки / Под ред. Мухина В. И.— М.: РВСН, 1992

Технический шпионаж и борьба с ним.— Минск: ТГО, 1993.

Технология электронных коммуникаций. Безопасность в телекоммуникационных сетях. — М, 1992. т. 20.

Тигулев Максим. Стеганозавр или Тайнопись на компьютере. // Интернет № 3, 1998.

Трушина Е. А. Идентификация пользователя ЭВМ по клавиатурному почерку как метод защиты от несанкционированного доступа. 1997. www.securityclub.ru

Уилл Найт. Взломан шифр нового типа. «Экономика и жизнь Кузбасса». www.mega.kemerovo.su

Устройства дактилоскопического доступа в помещение. http://www.rinnai.ru/room.htp

Фланаган Дж. Анализ, синтез и восприятие речи. — М.: Связь, 1968. — 392с.

Фролов А. В., Фролов Г. В. Осторожно: компьютерные вирусы. ЦМ.: ДИАЛОГ-МИФИ, 1996. — 256 с.

Хакимова Е. Террор с электронным лицом. // Мир новостей, № 14, 2001. http://www.sbf.ru/company.phtml?id=81.

Ховард Миллман. Не бойтесь технологий, вышедших из недр секретных служб. InfoWorld, США. // Computerworld № 27. —1998.

Хомяков Е.И., Федоров В.М. Стеганография данных с помощью речевых сообщений. ТРТУ г. Таганрог // http://old.tsure.ru:8101/UNIVERSITY/FIB/DIT/rus/seminar/44.html

Хори Д. Усовершенствуй свой телефон / Пер. с англ.— М.: БИНОМ, 1995. — 305 с.

Хорст Файсель. Криптография и компьютерная безопасность. — перевод А. Винокурова. http//security.nsys.by/

Хофман Л. Д. Современные методы зашиты информации. М—: Сов. Радио, 1980.

Хроника вирусного вредительства. // Компьютер-информ, № 13, июль 2000.

Хроника вирусования. // Компьютер-информ, №13, июль 2000.

Цыгичко В.Н., Черешкин Д. С., Смолян Г. Л. Защита гражданского общества от информационного оружия в XXI веке. // http://www.fbr.donetsk.ua/InfoWar/.

Черешкин Д. С., Смолян Г. Л., Цыгичко В. Н. Реалии информационной войны.// http://www.fbr.donetsk.ua/InfoWar/.

Хакимова Е. Террор с электронным лицом. // Мир новостей, ¹ 14, 2001. http:// www.sbf.ru/company.phtml?id=81.

Ховард Миллман. Не бойтесь технологий, вышедших из недр секретных служб. InfoWorld, США. // Computerworld ¹ 27. —1998.

Хомяков Е.И., Федоров В.М. Стеганография данных с помощью речевых сообщений. ТРТУ г. Таганрог // http://old.tsure.ru:8101/UNIVERSITY/FIB/DIT/rus/seminar/44.html

Хори Д. Усовершенствуй свой телефон / Пер. с англ.— М.: БИНОМ, 1995. — 305 с.

Хорст Файсель. Криптография и компьютерная безопасность. — перевод А. Винокурова. http//security.nsys.by/

Хофман Л. Д. Современные методы зашиты информации. М—: Сов. Радио, 1980.

Хроника вирусного вредительства. // Компьютер-информ, ¹ 13, июль 2000.

Хроника вирусования. // Компьютер-информ, ¹13, июль 2000.

Цыгичко В.Н., Черешкин Д. С., Смолян Г. Л. Защита гражданского общества от информационного оружия в XXI веке. // http://www.fbr.donetsk.ua/InfoWar/.

Черешкин Д. С., Смолян Г. Л., Цыгичко В. Н. Реалии информационной войны./ / http://www.fbr.donetsk.ua/InfoWar/.

Численные методы Н. С. Бахвалов. Главная редакция физико-математической литературы изд-ва «Наука», М., 1975. — 631с.

Шарат Панканти, Рууд М.Болле, Энил Джейн. Биометрия: будущее идентификации. // Открытые системы, ¹ 3 — 2000.

Широчкин В. П., Кулик А. В, Марченко В. В. Динамическая аутентификация на основе анализа клавиатурного почерка. // Информатика, управление и вычислительная техника., ¹ 32. Киев. 1999.

Эндрю Конри-Мюррей. Не самые секретные составляющие сетевой безопасности. // LAN / Журнал сетевых решений. — Сентябрь 2001.

Энн Харрисон. Запланированный взлом ключа ECC. // Computerworld ¹ 18 — 2000. http://www.osp.ru/cw/2000/18/040_0.htm

Яновский М. Как выбрать источник питания.

Ярочкин В. И. Технические каналы утечки информации. — М.: ИПКИР, 1994.

Ярочкин В. Проблемы информационной безопасности. Частный сыск и охрана. 1993.— ¹ 9.

Carlo Kopp. The E-bomb — a Weapon of Electronical Mass Destruction. Information Warfare: Thunder's month press, New York, 1996.

David A. Fulghum. Microwave Weapons Await a Future War. Aviation Week and Space Technology, June 7, 1999.

Winn Schwartau. More about HERF than some? Information Warfare: Thunder's month press, New York, 1996.

ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ